



**TEKNIikka JA LIKENNE**

**Tietotekniikka**

**Tietoverkot**

**INSINÖÖRITYÖ**

**KOTIKÄYTTÖÖN SOPIVA ASTERISK-PUHELINVAIHDE**

**Työn tekijä: Mikko Sahlberg**

**Työ hyväksytty: \_\_\_\_ . \_\_\_\_ . 2010**

**Marko Uusitalo  
lehtori**



## **ALKULAUSE**

Tämä insinööriö tehtiin henkilökohtaisena projektina Metropolia Ammattikorkeakouluun. Kiitän kaikkia tämän projektin toteuttamiseen osallistuneita testaaajia, laitteiden lainaajia, järjestelmän käyttäjiä ja puskaradiota.

Helsingissä 25.1.2010

Mikko Sahlberg

## TIIVISTELMÄ

<b>Työn tekijä:</b> Mikko Sahlberg	
<b>Työn nimi:</b> Kotikäyttöön sopiva Asterisk-puhelinvaihde	
<b>Päivämäärä:</b> 25.1.2010	<b>Sivumäärä:</b> 62 s. + 5 liitettä
<b>Koulutusohjelma:</b> Tietotekniikka	<b>Suuntautumisvaihtoehto:</b> Tietoverkot
<b>Työn ohjaaja:</b> lehtori Marko Uusitalo	
<p>Tässä insinöörityössä tutkittiin ystävien ja sukulaisten käyttöön tulevan Asterisk-puhelinvaihteen konfigurointia, asennusta ja käyttöönottoa. Työ tehtiin tekijän omana projektina. Työn tavoitteina oli asentaa täysin toimiva puhelinvaihde, johon käyttäjät pystyvät kirjautumaan mistä tahansa. Puhelinvaihteesta täytyi pystyä soittamaan julkiseen puhelinverkkoon ja käyttäjien tuli pystyä ryhmäkeskusteluun puhelinkonferenssia käyttäen. Aikaan saatu puhepalvelin yhdistettiin julkiseen puhelinverkkoon GSM-päätelaitteella.</p> <p>Työn teoriaosuus koostuu kahdesta osasta. Ensimmäisessä tutkitaan julkisen puhelinverkon arkkitehtuuria ja tekniikoita. Näitä tekniikoita olivat TDM-kanavointi, ISDN-liittymät ja puhelinverkon numerointi. Toisessa teoriaosiossa tutkittiin VoIP-puhelut mahdollistavia IP-pohjaisen dataverkon protokollia ja tekniikoita, kuten SIP- ja IAX-merkinantoprotokollia, RTP/RTCP-reaaliaikaisen median siirtoprotokollat, QoS-tekniikoita ja puhekoodekeja.</p> <p>Työssä käydään läpi järjestelmän asentaminen käyttäen AsteriskNOW-asennuspakettia ja tutkitaan ohjelmiston komponentteja. Tämän jälkeen keskitytään Asterisk konfigurointia, CounterPath X-lite ohjelmistopuhelimien asentamiseen, Ericsson Dialog 4422 IP-puhelimen asentamiseen ja Cisco Systems ATA 186-puhelinsovittimen asentamista.</p> <p>Työssä asennettiin Nokia 22 PBX GSM-päätelaite, joka oli kytketty Ciscon ATA-sovittimeen. Järjestelmästä soitettavia puheluita analysoitiin, ja puheluiden laatu todettiin hyväksi, mutta puheluisissa oli hieman viivettä A-tilaajalta B-tilaajalle. Verkkoa haluttiin parantaa tutkimalla, mitä verkkopalveluita VoIP-verkkoon voidaan asentaa ja miten ne auttavat verkon toimintaa. Käsiteltyjä protokollia olivat DHCP, NTP, TFTP ja HTTP. VoIP-verkon tietoturva huomattiin yhdeksi olennaisimmista asioista, joten työssä haluttiin tutkia mahdollisia riskejä, palomuurien rooleja ja puhepalvelimen tietoturvan parantamista. Työssä päästiin kaikkiin sen tavoitteisiin ja työn toteuttaminen tuntui työn tekijästä hyvin opettavalta.</p>	
<b>Avainsanat:</b> Asterisk, VoIP, SIP, RTP, Puhelinvaihde	

## ABSTRACT

<b>Name:</b> Mikko Sahlberg	
<b>Title:</b> Asterisk as a home PBX	
<b>Date:</b> 25.1.2010	<b>Number of pages:</b> 62 + 5 appendices
<b>Department:</b> Information Technology	<b>Study Programme:</b> Data Networks
<b>Instructor:</b> Marko Uusitalo	
<p>This final project studies installation, configuration and implementation of an Asterisk PBX as home PBX system. Users were friends and family. This project was done as a personal project. Objectives of this study were to install fully operational PBX, which can be accessed from anywhere. The PBX had to be able to make external calls to PSTN and users had to be able access a conference bridge. After implementation the PBX was connected to the cellular network using GSM gateway.</p> <p>Theoretical part of this study was divided to two sections. One of the sections of this study examines PSTN architecture and technology such as TDM, ISDN and PSTN numbering. Another section studies protocols and technologies that make it possible to transfer calls over IP data network such as SIP and IAX signalling protocols and RTP/RTCP real-time media transmission, QoS and audio codecs.</p> <p>This study went through installation process of AsteriskNOW installation package and studies the components of Asterisk system. After the installation this study focuses on configuration of Asterisk and the installations of Counter Path X-lite soft phone, Ericsson Dialog 4422 IP-phone and Cisco Systems ATA 186 phone adapter. The Nokia 22 PBX GSM gateway which was used in this study was connected to Cisco ATA phone adapter.</p> <p>The PBX was tested and analysed. This study confirmed phone calls to be of good quality. However there was some delay between A- and B-party. This study also examines how to develop VoIP enabled data network and which network services are useful for VoIP. Following protocols were examined DHCP, NTP, TFTP and HTTP. Network security of VoIP network is mandatory, therefore this study researches possible threats, role of the firewall and improving of PBX security. All the goals were met and this study was discovered to be very educational for author.</p>	
<b>Keywords:</b> Asterisk, VoIP, SIP, RTP, PBX	

# SISÄLLYS

## ALKULAUSE

## TIIVISTELMÄ

## ABSTRACT

<b>1. JOHDANTO</b>	<b>1</b>
<b>2. PUHELINVERKKO</b>	<b>2</b>
2.1. Tiedonsiirto, merkinanto ja kytkennät	2
2.2. Julkinen puhelinverkko	3
2.3. Aikajakokanavointi	6
2.4. ISDN	7
2.5. Numerointi	8
2.6. Puhelinvaihdoverkko	9
<b>3. VOIP</b>	<b>11</b>
3.1. VoIP-verkko	11
3.2. SIP	13
3.3. Median siirto	17
3.4. Inter-Asterisk eXchange	19
3.5. Palvelun laatu	19
3.6. Puheen koodaus	21
<b>4. ASTERISK</b>	<b>22</b>
4.1. Vaatimukset	23
4.2. AsteriskNOW-asennus	24
4.3. Hakemistot, tiedostot ja komentotulkki	25
<b>5. KONFIGUROINTI</b>	<b>27</b>
5.1. Numeroanalyysi	27
5.2. SIP-kanavat	29
5.3. ATA-sovitin	33
5.4. AGI- ja AMI-rajapinnat	35
5.5. Puhekonferenssi ja puheposti	36

<b>6. GSM-PÄÄTELAITE</b>	<b>37</b>
6.1. Nokia 22 PBX	38
6.2. Asennus ATA-sovittimeen	41
6.3. Toiminnan testaus ja analysointi	43
6.4. Hätäliikenneohjaukset	48
<b>7. PALVELIMEN VERRKOPALVELUT</b>	<b>51</b>
7.1. HTTP	51
7.2. DHCP	51
7.3. NTP	52
7.4. TFTP	53
<b>8. TIETOTURVA</b>	<b>53</b>
8.1. Mahdolliset uhat	53
8.2. Palomuuuri	55
8.3. Puhepalvelimeen tietoturva	57
8.4. Puheluiden salaus ja verkkoelementtien tietoturva	59
<b>9. YHTEENVETO JA TULEVAT PROJEKTIT</b>	<b>60</b>

## **VIITELUETTELO**

## **LIITTEET**

LIITE 1. SIP-vastauskoodit

LIITE 2. Ericsson Dialog 4422 IP:n konfiguraatitiedosto

LIITE 3. Cisco Systems ATA 186-sovittimen aloituskonfigurointi

LIITE 4. Cisco Systems ATA 186-sovittimen konfiguraatit

LIITE 5. SIP-merkinantoviestit soittaessa ohjelmistopuhelimesta matkapuhelimeen

ACD	Automatic Call Diversion. Puhelinvaihteiden palvelu, jolla ohjataan puheluita automaattisesti.
ACL	Access Control List. Estotaulukko, joita käytetään palomuureissa estämään haitallista liikennettä pääsemästä verkkoon.
DHCP	Dynamic Host Configuration Protocol. IP-osoitteiden automaattiseen jakamiseen käytetty protokolla.
Diffserv	Differentiated Service. QoS-tekniikka, jolla IP-paketit priorisoidaan liikenteen tyyppin perusteella.
DISA	Direct Inward System Access. Puhelinvaihteen palvelu, jonka avulla puhelinvaihteeseen voidaan kirjautua ulkoisesta numerosta.
DTMF	Dual-Tone Multi-Frequency. Puhelinlaitteiden käyttämä ääni-taajuusvalintatapa.
ETSI	European Telecommunications Standards Institute. Eurooppalainen telealan standardoimisjärjestö.
E&M	Earth&Magneto tai Ear&Mouth. Tasavirtaan perustuva analoginen merkinanto, jota käytetään puhelinkeskusten ja puhelinvaihteiden yhteyksissä.
FXO	Foreign eXchange Office. Puhelinrajapinta, joka vastaanottaa soittojännitettä ja valintaääntä.
FXS	Foreign eXchange Station. Puhelinrajapinta, joka toimii jännitelähteenä sekä lähettää valintaääntä ja soittojännitettä.
GNU	GNU's Not Unix. Projekti, jossa tavoitteena on kehittää täydellinen vapaa käyttöjärjestelmä.
GPL	GNU General Public License. Vapaa ohjelmistolisenssi.
HSCSD	High Speed Circuit Switched Data. GSM-verkossa käytetty dataliikenteen siirtotekniikka.
IETF	Internet Engineering Task Force. Internet-protokollien standardoinnista vastaava organisaatio.
ISUP	ISDN User Part. Osa SS7-merkinantoa.
ISDN	Integrated Services Digital Network. Piirikytkentäisen puhelinverkon järjestelmä.
ISDN BRI	ISDN Basic Rate Interface. ISDN-perusliittymä.
ISDN PRI	ISDN Primary Rate Interface. ISDN-järjestelmäliittymä.
ITU	International Telecommunication Union. Kansainvälinen televiestintäliitto.
LAN	Local Area Network. Lähiverkko.
MPLS	Multi Protocol Label Switching. Dataverkon reititys tekniikka.
NAT	Network Address Translation. IP-osoitteen muunnokseen käytetty tekniikka.

PoE	Power over Ethernet. Verkkokaapelissa sähkön jakoon käytetty tekniikka.
QoS	Quality of Service. Tietoliikenneverkon priorisointi ja luokittelu.
RTP	Real-time Transport Protocol. Median siirtoon käytetty protokolla.
SDP	Session Description Protocol. SIP-merkinantoprotokollan apuna käytettävä protokolla, joka kuvaa muodostettavia istuntoja.
SIP	Session Initiation Protocol. IP-verkon merkiantoprotokolla.
SRTP	Secure Real-time Transport Protocol. Salatun median siirtoon käytetty protokolla.
STUN	Session Traversal Utilities for NAT. Realiaikaisen puhe ja videoliikenteen NAT-muunnoksia varten kehitetty protokolla.
SS7	Signaling System 7. Puhelinverkossa käytetty runkoverkon merkinantoprotokolla.
SSL	Secure Sockets Layer. IP-liikenteen salausprotokolla nykyään tunnetaan nimellä TLS.
TDM	Time-division Multiplexing. Aikajakokanavointi.
TLS	Transport Layer Security. IP-liikenteen salausprotokolla, joka kehitettiin SSL:stä.
VoIP	Voice over Internet Protocol. Puheluiden siirtämiseen dataverkossa käytetty tekniikka.
VLAN	Virtual Local Area Network. Lähiverkon loogiseen jakoon käytetty tekniikka.
WAN	Wide Area Network. Laajaverkko.



## 1. JOHDANTO

Tässä insinööriyössä tutkittiin, suunniteltiin ja asennettiin kotikäyttöön sopiva Asterisk-puhepalvelin, jonka käyttäjäkunta koostuu ystäväistä ja sukulaisista. Vastaava puhelinjärjestelmä voisi olla pienyrityksen tai taloyhtiön käytössä. Työ tehtiin omana projektina, joten puhepalvelimen laitteisto kerättiin kaasaan vanhoista tietokoneen osista, joita oli kerääntynyt nurkkiin. Työ toteutettiin puhelinlaskujen vähentämiseksi ja helpottamaan käyttäjien välistä viestintää. Tavoitteena on: saada käyttäjät kirjautumaan puhepalvelimelle omalta kotikoneeltaan, puhepalvelimesta tulee pystyä soittamaan ja vastaanottamaan ulko- ja sisäpuheluita sekä käyttäjien täytyy pystyä ryhmäkeskusteluun puhelinkonferenssin avulla.

Tämä insinööri työ painottuu työn toteuttamisen kannalta olennaisiin asioihin, mutta näiden asioiden lisäksi tässä työssä esitellään vaihtoehtoisia reittejä, joihin vastaavaa järjestelmää voisi lähteä kehittämään. Työ sisältää teoriaosuuden, jossa esitellään työssä käytetyt protokollat ja tekniikat. Samalla pyritään laajentamaan lukijan näkemystä, miten ja mistä puhelut kulkevat. Teoriaosuus on jaettu kahteen osaan, joista ensimmäisessä perehdytään puhelintekniikan perusteisiin, puhelinverkkojen arkkitehtuuriin ja rakentamiseen. Toisessa osassa vuorostaan käsitellään IP-pohjaisen pakettikytkentäisen dataverkon yli siirrettävien VoIP-puheluiden vaatimuksia ja ominaisuuksia sekä olennaisia protokollia ja tekniikoita.

Työn käytännönosuus lähtee käyntiin palvelimen laitteistovaatimusten selvittämisellä ja itse puhepalvelimen asennuksella. Tämän jälkeen syvennyttään Asterisk-puhelinvaiheohjelmistoon, joka hoitaa puheluiden ohjausta ja kytkentää. Seuraavaksi selvitetään miten asennettu puhepalvelin voidaan yhdistää julkiseen puhelinverkkoon. Tässä työssä liittymänä käytettiin GSM-päätelaitetta, joka osaa ohjata ja vastaanottaa puheluita matkapuhelinverkosta.

Onnistuneen asennuksen jälkeen esitellään käytetyt puhelimet ja niiden konfiguraatiot sekä analysoidaan ja mitataan järjestelmän toimivuutta. Tämän jälkeen syvennyttään, mitkä verkkopalvelut ovat VoIP-verkossa olennaisia. Lopuksi analysoidaan asennetun VoIP-verkon tietoturva sekä tutkitaan, mitä ja miten tietoturva voitaisiin parantaa vastaamaan palvelimen käyttötarkeitusta.

Tästä kirjallisesta tuotoksesta pyrittiin kirjaamaan ylös Asterisk-palvelimen asentamisen ja ylläpidon kannalta olennaisia asioita. Tästä syystä kirjallisessa tuotoksessa keskityttiin niihin palveluihin ja ominaisuuksiin, joita asennetussa järjestelmässä on käytössä.

## **2. PUHELINVERKKO**

Tässä osiossa esitellään työn kannalta olennaisia asioita ja osia puhelinverkosta. Puhelinverkko koostuu puhelinkeskuksista, joilla verkon eri alueet yhdistetään toisiinsa, ja verkon käyttäjistä, joita kutsutaan tilaajiksi. Soittavaa osapuolta kutsutaan A-tilaajaksi ja puhelua vastaanottavaa tilaajaa B-tilaajaksi. A- ja B-tilaajan välinen puhelu voidaan toteuttaa monella eri tavalla, joten tässä osiossa esitellään puhelun muodostumista varten tarvittavat komponentit, kiinteän puhelinverkon verkkoelementit, matkapuhelinverkkoon verkkoelementit ja puhelinvaihdoverkon perusteet. [1, s. 19 – 22.]

### **2.1. Tiedonsiirto, merkinanto ja kytkennät**

Kaiken tyyppiset tietoliikenneverkot vaativat vähintään kolme eri operaatiota, joilla verkon tilaajien välinen yhteys ja tiedonsiirto voidaan toteuttaa. Nämä kolme operaatiota ovat tiedonsiirto, merkinanto ja kytkentä. Tiedonsiirrolla tarkoitetaan kahden pisteen välillä tapahtuvaa analogisen tai digitaalisen signaalin siirtoa tiedonsiirtokanavaa pitkin. Tiedonsiirto koostuu kolmesta peruselementistä lähettimestä, joka lähettää signaalia, lähetyskanavasta, joka on muodostettu fyysiseen mediaan ja vastaanottimesta, joka vastaanottaa lähetettyä signaalia. Fyysisenä mediana käytetään esimerkiksi kuparista valmistettua parikaapelia, valokuitukaapelia tai radioaaltojen käyttämää ilmarajapintaa. [1, s. 20, s. 125 – 127.]

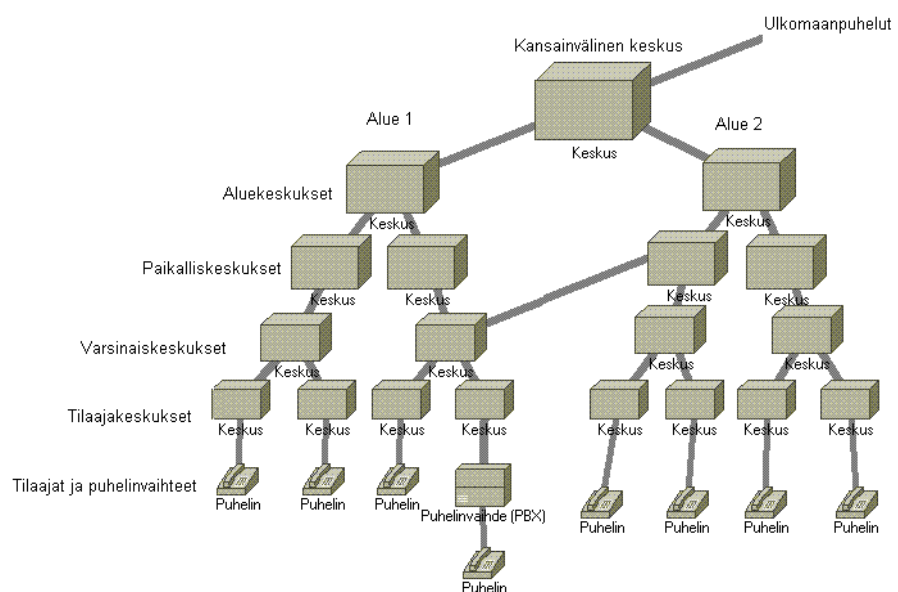
Signalointi, eli merkinanto operaatioita käytetään verkkolaitteiden välisen yhteyden muodostamiseen, hallintaan ja purkamiseen. Merkinannolla verkkolaitteet keskustelua keskenään, jotta käyttäjät pystyisivät keskustelemaan keskenään. Merkinantotekniikoita ja protokollia on useita, mutta ne voidaan jakaa kahteen pääryhmään liityntäverkon- ja runkoverkonmerkinantoon. Liityntäverkonmerkkiannossa verkon yhdyskäytävä, kuten puhelinkeskus ja siihen kytketty tilaaja, signaloivat toistensa välillä, kun taas runkoverkon merkinannossa kaksi verkon yhdyskäytävää signaloivat toistensa välillä. [2, s. 426 – 427.]

Kytkenällä tarkoitetaan tietoliikenneverkossa yhteyksien ohjaamista ja muodostamista. Kytkentää tulee tehdä jonkun yksilöllisen identiteetin perusteella. Esimerkiksi puhelinverkossa puheluiden ohjaamista tehdään puhelinnumeron perusteella. Puhelinverkko jaetaan numeron perusteella numeroalueisiin ja jokaisesta numeroalueesta vastaa tietty puhelinkeskus, johon numeroalueen tilaajat on kytketty. Keskukset yhdistetään toisiinsa ja ne konfiguroidaan ohjaamaan puheluita toisilleen puhelinnumeron perusteella. Näin keskukset pystyvät ohjaamaan ja yhdistämään puheluita numeron perusteella tilaajalta toiselle. [3, s. 73 – 76.]

## 2.2. Julkinen puhelinverkko

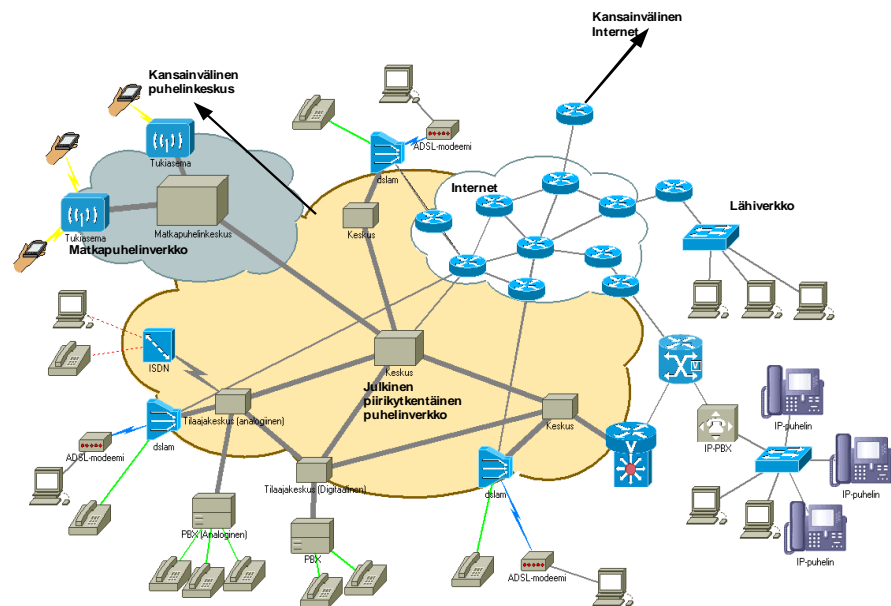
Julkinen puhelinverkko sisältää kiinteän piirikytkentäisen puhelinverkon ja matkapuhelinverkon. Kiinteäpuhelinverkko muodostuu keskuksista, sekä verkon tilaajista. Kiinteäpuhelinverkon tilaajat voivat olla ISDN BRI-tekniikkaa hyväksikäyttäviä digitaalisia puhelimia, IP-puhelimia tai yleensä DTMF-merkinantoa käyttäviä analogisia puhelimia [4, s. 12].

Puhelinverkon kysyntä kasvaa, joten sen keskukset tulee jakaa kytkentähierarkia tasoihin sen perusteella kuinka paljon tilaajia niiden lähistöllä sijaitsee. Kuvassa 1 on esitelty tyypillinen valtakunnallisen kiinteäpuhelinverkon kytkentähierarkia. Eri alueet voidaan myös yhdistää toisiinsa alemman hierarkiatason keskuksissa, vaikka kuvassa 1 alueiden väliset puhelut kulkevat pääasiassa kansainvälisen keskuksen kautta.



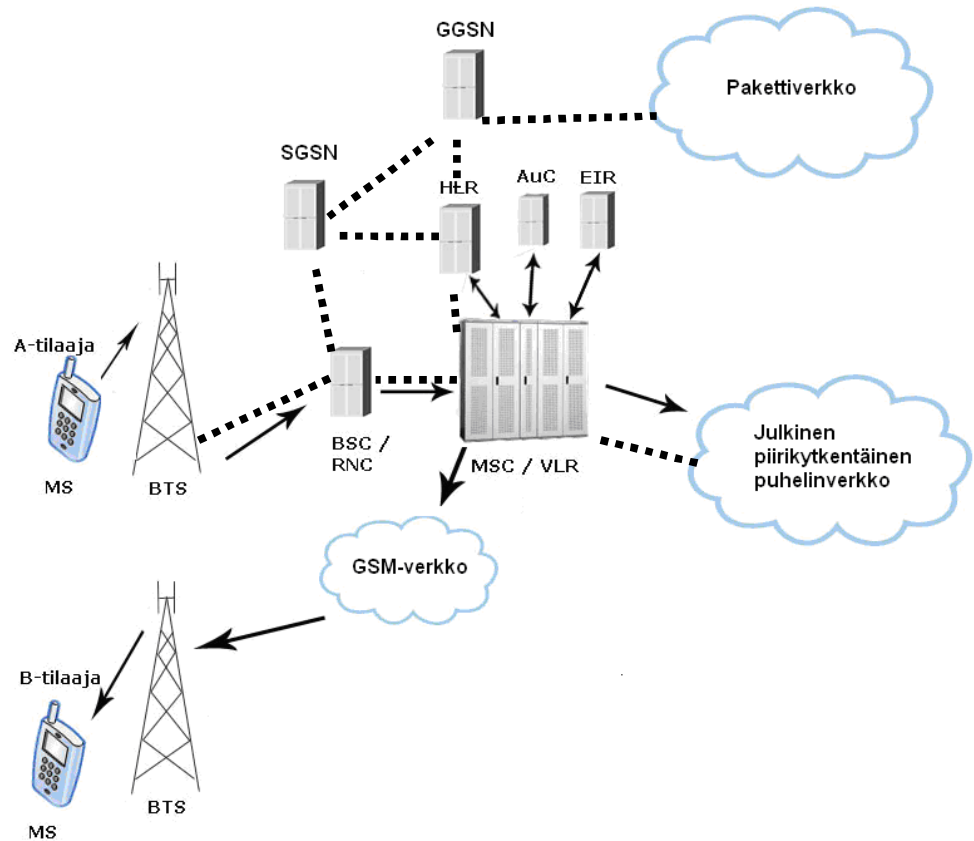
Kuva 1. Kiinteäpuhelinverkon keskushierarkia [1].

Kiinteä puhelinverkko on myös yhdistetty muihin tietoliikenneverkkoihin, kuten matkapuhelinverkkoon, Internetiin ja eri puhelinvaihteverkkoihin. Käyttäjien kannalta on järkevää, että samalla päätelaitteella voi ottaa yhteyden muihin verkkoihin. Ei olisi järkevää, jos käyttäjän pitäisi vaihtaa päätelaitetta aina, kun soittaa eri tietoliikenneverkon tilaajalle, joten tilaajat pitää pystyä tavoittamaan, vaikka ne sijaitsevat kiinteänverkon ulkopuolella. Kuvassa 2 on suurpiirteinen kuva nykyajan piiriyhteyksistä puhelinverkosta.



Kuva 2. Julkinen piiriyhteyksinen puhelinverkko [1. s. 57].

Kuten kuvasta 2 nähdään, julkisessa piiriyhteyksisessä puhelinverkossa on käytössä monia eri tekniikoita. Tilaajat voivat olla ISDN-perusliittymiä käyttäviä kotitalouksia, joiden Internet ja puhelinliikenne kulkee samojen ISDN-piirien yli. Nykyään yleisempi yhteystekniikka on laajakaistayhteys DSL eli digitaalinen tilaajayhteys, jolloin samassa fyysisessä mediassa kulkee Internet ja puhelinliikenne. Data- ja puhelinliikenne erotellaan toisistaan DSL-keskittimellä, eli DSLAM:llä. Yritykset ja muut organisaatiot käyttävät puhelinvaihteita, joiden avulla luodaan organisaation sisäinen puhelinverkko. Puhelinvaihteet voivat olla analogisia, digitaalisia tai IP-puhelinjärjestelmiä, joten niiden käyttämät liityntäteknikat vaihtelevat, mutta yleisimmin käytössä on ISDN S2 PRI liittymä.



Kuva 3. Matkapuhelinverkko [5, s. 121 – 122, s. 176, s. 210].

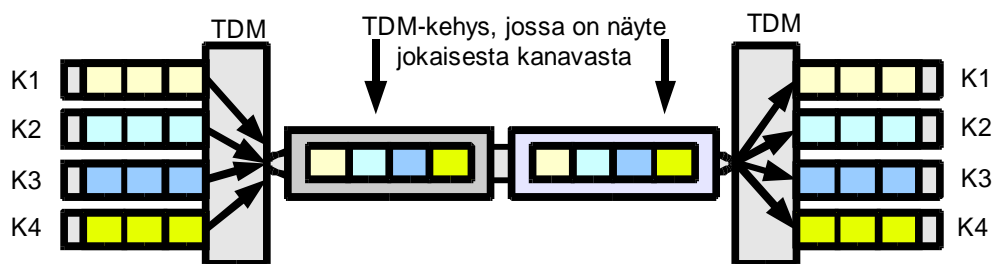
Kuvassa 3 on esitelty, miten puhelu (viiva) ja data (katkoviiva) kulkee matkapuhelinverkon verkkoelementtien välillä. Matkapuhelinverkko käyttää radiotekniikkaa matkapuhelimen ja verkon väliseen kommunikointiin. Verkko on jaettu radiosoluihin, joiden alueella olevia tilaajia tukiasemat palvelevat. [5, s. 114 – 122.] Matkapuhelinverkon verkkoelementtejä on useita ja niiden tehtäviä on esitelty alla:

- MS (Mobile Station) eli liikkuva päätelaite kuten matkapuhelin [5, s. 114 – 122].
- BTS (Base Transceiver Station) eli tukiasema vastaa yhden tai useamman radiosolun tilaajien digitaalisen liikenteen moduloinnista radiotietä varten, tiedon koodauksesta ja purkamisesta, sekä puheluiden salauksesta [5, s. 122 – 125].
- BSC (Base Station Controller) eli tukiasemaohjain vastaa siirtotien käytöstä, radiotien tiedonsiirtokanavista, itse radiosignaalista ja tilaajan liikkumisesta solusta toiseen. [5, s. 122 – 125.]
- RNC (Radio Network Subsystem) on UMTS-verkon tukiasema eli hoitaa tukiaseman tehtäviä 3G-puheluiden osalta [5, s. 210 – 211].

- MSC (Mobile Switching Center) eli matkapuhelinkeskus hoitaa puheluiden kytkentää, reititystä, tilaajien seurantaa ja toimii yhdyskäytävänä kiinteään verkkoon [5, s. 122 – 125].
- SGSN (Serving GPRS Support Node) on laite, joka seuraa GPRS-laitteita, reitittää näille tulevaa ja näiltä lähtevää liikennettä sekä huolehtii liikenteen salaamisesta. Tämän lisäksi SGSN kerää laskutukseen liittyviä tietoja [5, s. 175 – 177.].
- GGSN (Gateway GPRS Support Node) toimii yhdyskäytävänä matkapuhelinverkon ulkopuoliseen pakettikytkentäiseen verkkoon [5, s. 175 – 177].
- HLR (Home Location Register) eli kotirekisteri pitää kirjaa koko verkon tilaajien tiedoista, sijainnista verkossa ja palveluista [5, s. 124 – 125].
- VLR (Visitor Location Register) eli vierailijarekisteri sisältää tiedot oman alueensa tilaajista [5, s. 124 – 125].
- AuC (Authentication Center) eli tunnistuskeskus hoitaa puheluiden suojaukseen ja tietoturvaan liittyviä toimintoja [5, s. 124 – 125].
- EIR (Equipment Identity Register) eli laitetunnusrekisteri sisältää tietoa itse puhelinlaitteista esimerkiksi, mitkä laitteet eivät saa käyttää verkkoa [5, s. 124 – 125].

### 2.3. Aikajakokanavointi

Synkroninen aikajakokanavointi (TDM) on yleisin puhelinverkossa käytetty kanavanjakotekniikka, jolloin jokaiselle tilaajalle varataan oma aikaväliksi kutsuttu tiedonsiirtokanava. Aikaväli voi olla tietyn mittainen tai vaihtelevan mittainen ja sen aikana saatetaan lähettää vain osa koko lähetettävästä sanomasta. Kiinteässä tietoliikenneverkossa aikajakokanavointi toimii tehokkaasti, mutta langattomissa tietoliikenneverkoissa päätelaitteiden synkronoinnin kanssa tulee ongelmia [6, s. 72]. Aikavälit voidaan jakaa tilaajien kesken esimerkiksi siten, että kaikki tilaajat lähettävät tietoa kerrallaan enintään 40 ms ajan. Tilaaaja A lähettää tietoa hetkellä  $t$ , tilaaaja B hetkellä  $t+40$  ms, tilaaaja C hetkellä  $t+80$  ms ja tilaaaja D hetkellä  $t+120$  ms. Kaikkien tilaajien lähetettyä tietoa kerran aloitetaan kierros alusta. Näitä kierroksia kutsutaan TDM-kehyksiksi. [6, s.73 – 74, s. 329 – 338.]



Kuva 4. Aikajakokanavointi [6, s. 74].

Kuvassa 4 näkyy, miten tilaajien liikenne siirretään aikajakokanavointia käyttäen päätepisteestä toiseen. Tilaajien lähettämä liikenne pakataan TDM-kehyksiin, jokainen omaan aikaväliinsä ja siirretään samaa fyysistä mediaa käyttäen toisen päätepisteeseen, missä kehykset puretaan ja jokaisen aikavälin liikenne ohjataan oikeaan osoitteeseen.

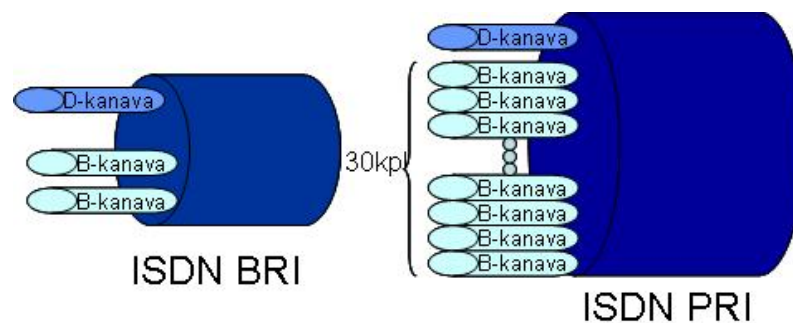
## 2.4. ISDN

ISDN on digitalisoidussa puhelinverkoissa käytetty aikajakokanavointiin perustuva tilaajaliittymäteknikka. ISDN-rajapintoja on useisiin eri tarkoituksiin ja sille on määritelty useita eri kanavoita. ISDN-tekniikka on standardoinnista huolimatta kehittynyt moneen suuntaan, sillä useat laitevalmistajat alkoivat kehittää ISDN-tekniikkaa omien tuotteittensa kanssa paremmin yhteensopivaksi. ISDN on yhteensopiva monien muiden puhelinverkossa käytettyjen merkinantojen kanssa. Erityisesti ISUP-protokollan ansiosta ISDN-tilaajat pystyvät käyttämään kaikkia SS7-merkiannolla toteutetun puhelinverkon palveluita. [4, s. 64.] Tässä työssä esitellään vain olennaisimmat ISDN-kanavat ja liittymätyypit.

ISDN BRI eli ISDN-perusliittymä (ITU-T I.430) on kansainvälisen televiestintäliiton ITU:n televiestintäsektorin standardoima puhelinverkkojärjestelmä. ISDN-perusliittymällä on käytössä kaksi B-kanavaksi kutsuttua liikennekanavaa, joilla on käytössä 64 kbit/s kaistanleveyttä. B-kanavassa voidaan siirtää puheen lisäksi myös dataa ja faksiliikennettä, sekä videokuvaa. B-kanavan lisäksi perusliittymä käyttää yhtä D-kanavaksi kutsuttua merkinantokanavaa kaistanleveydeltään 16 kbit/s. ISDN-perusliittymän siirtonopeus on  $2 \cdot 64 = 128$  kbit/s, koska D-kanavaa ei voida käyttää liikenteen siirtoon. [4, s.12 – 13.]

ISDN PRI (ITU-T I.431) eli ISDN-järjestelmäliittymä toimii käytännössä samoin kuin ISDN BRI, mutta suuremmalla kaistanleveydellä. PRI:n nopeus

riippuu käytetyn TDM-kehyksen koosta, joka riippuu siitä, käytetäänkö T1- vai E1-kehystä. Euroopassa ja Suomessa käytetään E1-kehystä, joissa on yksi D-kanava ja 30 B-kanavaa, joten yhteenlaskettu kaistanleveys on  $30 \times 64 = 2,044$  Mbit/s. B-kanavien lisäksi E1-kehyksessä on synkronointi kanava 0 ja D-kanavalle on varattu aikaväli 16 [6, s. 337]. ISDN-järjestelmäliittymän D-kanavalla on käytössä 64 kbit/s kaistanleveyttä. T1-kehyksen siirtonopeus on 1,544 Mbit/s ja siihen mahtuu 23 B-kanavaa. Kuvassa 5 havainnollistetaan ISDN BRI- ja ISDN PRI-tekniikan eroa. [4, s.12-13.]



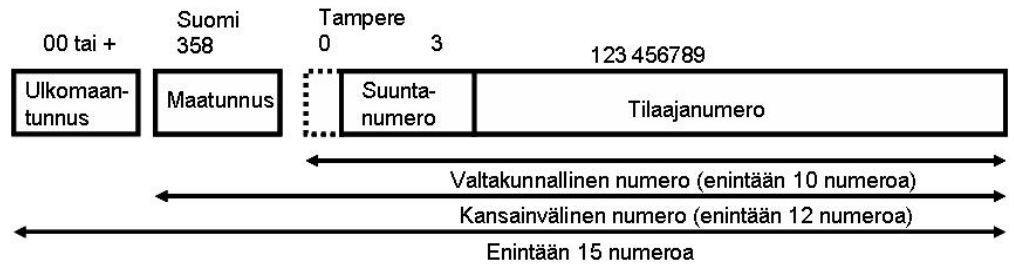
Kuva 5. ISDN BRI ja ISDN PRI. [4, s. 13.]

ISDN on datansiirtotekniikkana häviävä, koska sen siirtonopeus ei vastaa nykyajan kysyntää, mutta puhelinjärjestelmät käyttävät sitä edelleen paljon. Puhelinvaihteisiin kytketyt alaliittymät ovat usein laitevalmistajan omaa ISDN BRI-perusliittymää käyttäviä digitaalisia puhelimia. ISDN PRI-liittymillä muodostetaan yhteys puhelinvaihteen ja puhelinkeskuksen välille käyttäen S2-merkinantoa.

## 2.5. Numerointi

Numeroinnin ideana on jakaa tilaajat puhelinnumeron perusteella numeroalueisiin, jotka kertovat jotain tilaajista, kuten niiden maantieteellisen sijainnin. Esimerkiksi kaikki maat on eroteltu toisistaan maakohtaisiin numeroalueisiin käyttäen maatunnusta. Puhelinverkon numerointia varten on kaksi standardia NANP ja ITU-T E.164. ITU-T E. 164 on Euroopassa käytetty standardi. Se koostuu maatunnuksesta, suuntanumerosta ja tilaajanumerosta. Kuvassa 6 on esitelty ITU-T E.164 mukainen numerointi. [4, s.18 ; 1, s. 31 – 33.]





Kuva 6. ITU-T E.164 numerointi soitettaessa ulkomailta Tampereelle. [1, s. 31]

Maatunnus on yhdestä neljään numero ja sillä tunnistetaan valtio, jossa tilaaja sijaitsee. Suuntanumero on yhden tai kahden numeron pituinen tunnus, jossa on valtion sisällä soitettaessa 0-tunnus edessä. Suuntanumerolla tunnistetaan maan sisäinen numeroalue, esimerkiksi paikkakunta, jossa tilaaja sijaitsee. Maatunnus ja suuntanumero vaihtelevat riippuen maan numerointi tarpeista. Tilaajanumero on 1-9 numeroa pitkä numero, jolla tunnistetaan tilaaja. Koko puhelinnumero ei kuitenkaan saa olla yhteensä yli 15 numeroa pitkä. [1, s. 31 – 33.]

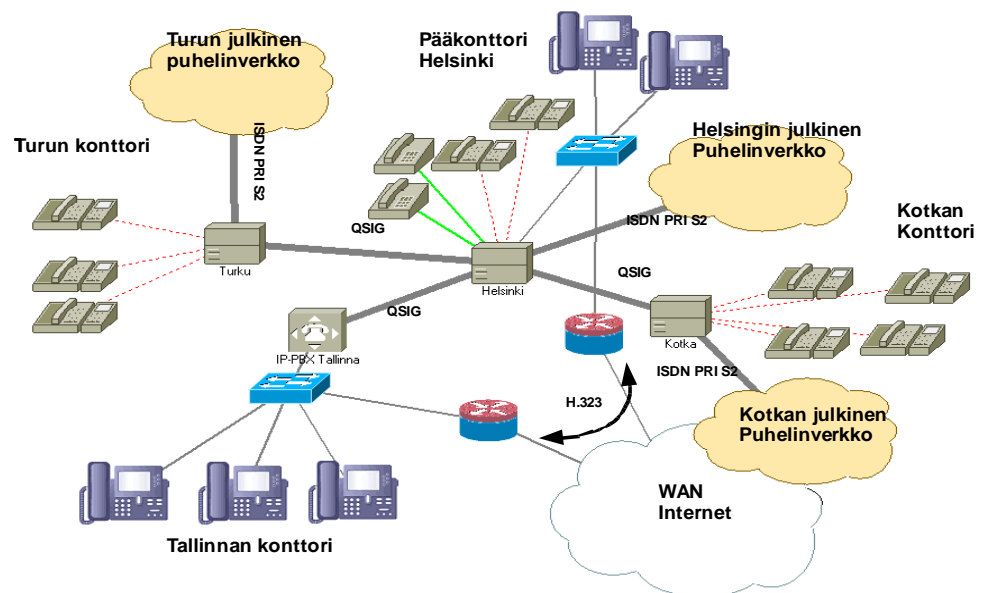
Soittaessa ulkomaille numeron eteen pitää lisätä ulkomaantunnus, joka usein on 00, mutta se vaihtelee maakohtaisesti. Suomessa teleoperaattoreiden kilpailun ansiosta 00-tunnuksen lisäksi, jokaisella operaattorilla on oma ulkomaantunnus 99x, jossa x määrittelee puheluun käytettävä operaattori. Matkapuhelinverkossa ulkomaan tunnus on +-merkki numeron edessä. [1, s. 31 – 33.]

## 2.6. Puhelinvaihdeverkko

Puhelinvaihdeverkko on organisaation oma puhelinverkko, joka koostuu pienistä puhelinkeskuksista eli puhelinvaihteista. Puhelinvaihteet ovat verrattavissa julkisen puhelinverkon keskuksiin ja puhelinvaihdeverkot toimivat hyvin samankaltaisesti kuin julkinen puhelinverkko. Suurimpia eroja ovat käytetyt merkinantoprotokollat, sillä ne ovat usein laitavalmistajien omia. Puhelinvaihdeverkkoja käytetään pääasiassa tietoliikennekustannusten vähentämiseksi, koska vaihdeverkon tilaajien väliset sisäpuhelut ovat ilmaisia. Puhelinvaihteita voidaan yhdistää toisiinsa puhelinvaihdeverkoksi käyttämällä siihen tarkoitettuja merkinantoprotokollilla, kuten QSIG. Puhelinvaihteiden käyttämät merkinantoprotokollat pystyvät siirtämään enemmän tietoa A- ja B-tilaajasta, kuin julkisen puhelinverkon merkinannossa. Maantieteellisesti toisistaan kaukana sijaitsevien puhelinvaihteiden välisille yhdyskäytävälle hanki-

taan julkisesta puhelinverkosta varattuja aikavälejä, joissa kulkee vain puhelinvaihteiden välistä liikennettä. Varattuista aikaväleistä muodostuu virtuaalisia yksityiseen käyttöön tarkoitettuja VPN-verkkoja, joille on varattu omat piirit julkisesta puhelinverkosta. Puhelinvaihteet pyrkivät tarjoamaan palveluita, joilla voidaan parantaa organisaation jäsenten välistä ja ulkopuolisten henkilöiden kanssa tehtävää kommunikaatiota. Yleisimpiä palveluita ovat tavoitettavuuspalvelu, jonka avulla tilaajat voidaan määritellä tavoittamattomiksi eri tiloihin esimerkiksi lomalla, lounaalla tai kokouksessa. Tavoitettavuus tilat ovat näkyvissä puhelunvälittäjille, jotka tiedottavat asiasta tavoittamattomalle tilaajalle soittaneelle henkilölle. Puhelinvaihteiden palvelut ovat suunniteltu liiketoimintaa harjoittaville yrityksille, joten niiden tehtävänä on parantaa henkilöstön saavutettavuutta. [4, s. 35 – 43.]

Keskuksen ja puhelinvaihteen välistä yhdyskäytävää kutsutaan keskusjohtoiksi, jotka ovat Suomessa yleensä digitaalisia ISDN-järjestelmäliittymiä S2-merkinantoa käyttäen. Vanhemmissa puhelinvaihteissa voi olla analogisia keskusjohtoja, jotka käyttävät R2-merkinantoa, mutta tämä rajoittaa puhelinvaihteen ominaisuuksia, koska tilaajasta ei saada siirrettyä yhtä paljon tietoa kuin ISDN-liittymää käytettäessä.



Kuva 7. Puhelinvaihteverkko.

Kuvassa 7 on esitetty esimerkki puhelinvaihteverkossa, jossa on neljä konttoria, joissa Tallinnan konttoria lukuun ottamatta on omat keskusjohdot. Keskusjohdot ovat kytketty paikalliseen julkiseen puhelinverkkoon, jotka ovat

paikallisten teleoperaattoreiden verkkoja. Konttorien puhelinvaihteet ovat yhdistettynä Helsingin päävaihteeseen QSIG-merkinantoa käyttävillä yhdyskäytävillä. Helsingin päävaihteeseen hoitaa konttoreiden välisten puheluiden ohjauksen ja ohjaa Tallinnasta tulevat puhelut oikean etuliitteen kanssa julkiseen puhelinverkkoon. Tallinnan konttorissa ei ole keskusjohtoja, koska sillä siellä sijaitsee puhelinasiakaspalvelukeskus, joten Tallinnan konttoriin tulee paljon puheluita, mutta sieltä lähtee vain vähän puheluita. Tallinnan IP-puhelinvaihteen liikenne ohjataan Helsingin päävaihteeseen QSIG-yhdyskäytävän lisäksi vaihtoehtoisesti Internetin yli kulkevalla H.323-yhdyskäytävällä.

Puhelinvaihteeseen kytketään puhelinkeskukseen keskusjohtoilla, jotka ovat yleensä digitaalisia ISDN-järjestelmäliittymiä S2-merkinantoa käyttäen. Vanhemmissa puhelinvaihteissa voi olla analogisia keskusjohtoja, jotka käyttävät R2-merkinantoa, mutta tämä rajoittaa puhelinvaihteen ominaisuuksia, koska tilaajasta ei saada siirrettyä yhtä paljon tietoa kuin ISDN-liittymää käytettäessä.

### 3. VOIP

Tässä osiossa käsitellään puheluiden toteuttamista dataverkossa ja sitä varten tarvittavia verkkoelementtejä. Voice over Internet Protocol on tekniikka, jolla puhetta voidaan siirtää IP-pohjaisessa pakettikytkentäisessä dataverkossa. VoIP sisältää kaksi perustoimintaa merkinantoprotokolla ja median siirto-protokolla. Merkinantoprotokollan tehtävänä on neuvotella, hallita, sekä purkaa yhteys A- ja B-tilaajan välillä. Median siirtoon käytettävän protokolla vastaa puhemedian siirrosta päätepisteestä toiseen dataverkon yli. Merkinantoprotokollia on useita, mutta tässä työssä perehdytään asennettavien laitteiden käyttämiin protokolleihin. Median siirto vuorostaan toteutetaan lähes aina käyttäen RTP- ja RTCP-protokollia, koska ne ovat tällä hetkellä tehtävään parhaiten soveltuva protokolla.

#### 3.1. VoIP-verkko

VoIP-verkon arkkitehtuuri vaihtelee suuresti riippuen verkossa käytettävästä merkinannosta, yhdyskäytävistä ja päätelaitteista. Päätelaitteina toimivat puhelimet voivat olla langallisia IP-puhelimia, mediayhdyskäytävän takana olevia digitaalisia tai analogisia lankapuhelimia, ohjelmistopuhelimia, IP DECT-

tukiasemia tai langattoman lähiverkon IP-puhelimia. Pääpiirteiltään verkot ovat kuitenkin samankaltaisia, koska vaikka merkinannosta riippuen verkossa tulee olla useita eri toimintoja toteuttavia palvelimia niiden toiminnot ovat integroitu samaan puhepalvelinohjelmistoon. [7, s. 73.]

IP-puhelimet voidaan yhdistää VoIP-verkkoon kiinteään IP-osoiteen tai DHCP-palvelimelta jaettavan dynaamisen IP-osoitteen avulla. IP-puhelimen numero voidaan sitoa IP-osoitteeseen tai MAC-osoitteeseen, mutta ne ovat usein kelluvia numeroita, joihin IP-puhelin kirjautuu käyttäjätunnuksella ja salasanalla. IP-puhelimille voidaan syöttää sähköä erillisen virtalähteen lisäksi käyttäen IEEE 802.3af standardin tai uudemman 802.3at standardin mukaisia PoE-kytkimiä. Ohjelmistopuhelimet ovat työasemiin asennettavia ohjelmistoja, jotka toimivat puhelimena. Ohjelmistopuhelimissa on usein paljon lisäominaisuuksia, kuten pikaviestintä- ja videopuhelusovelluksia. Ohjelmistopuhelimia voidaan asentaa työasemien lisäksi myös matkapuhelimiin, jolloin matkapuhelin toimii langattomassa lähiverkossa matkapuhelinverkon sijaan. Langattomat IP-puhelimet voivat olla langattomassa lähiverkossa liikkuvia WLAN-puhelimia tai DECT-puhelimia. [7, s. 76 – 79, s. 84.]

VoIP-verkkoon voidaan yhdistää langattomia puhelimia käyttäen IP-DECT-tukiasemia, jotka käyttävät SIP- tai H.323-merkinantoa tukiaseman ja puhepalvelimen välillä. Itse puhelimen ja tukiaseman väliseen yhteyteen käytetään eurooppalaisen telealan standardisointijärjestön ETSI:n standardoimaa langattoman puhelinverkon DECT-tekniikkaa. IP-DECT-järjestelmiä pidetään usein langatonta lähiverkkoa parempana vaihtoehtona yhdistää langattomia puhelimia VoIP-verkkoon. DECT-tekniikkaa pidetään parempana vaihtoehtona, koska DECT on piirikytkentäinen tekniikka, joten siinä ei tule viiveen ja viiveen vaihtelun kanssa ongelmia, joista WLAN-puhelimet kärsivät. DECT-puhelimien akut kestävät pidempään ja DECT toimii eri taajuusalueella kuin WLAN-tekniikat, joten DECT-puhelimet eivät ota häiriötä langattoman lähiverkon liikenteestä. [8, s. 246 – 248.]

Puhepalvelin on VoIP-verkon verkkoelementti, jonka tehtävänä on prosessoida puheluita tai suorittaa puheluihin liittyviä palveluita. Samaa puhepalvelimeen voidaan asentaa useita eri toimintoja kuten: puheluiden merkinanto, puheposti, puhelinluettelo tietokannat, Automatic Call Diversion palvelut, joita käytetään puheluiden automaattiseen ohjaamiseen esimerkiksi puherinkien ja puhesarjojen ohjaamisissa, automaattiset puhelunvälittäjät, puhe-

ja video sovellukset, konferenssit, sekä välityspalvelu. Näitä palveluita kuitenkin usein siirretään erillisille palvelimille, koska tilaajien lisääntyessä palveluiden suorittaminen vie liikaa resursseja puhepalvelimelta. [7, s. 72 – 73.]

Mediayhdyskäytävä on verkkoelementti, jonka tehtävänä on muuttaa merkinanto ja puhe- tai videomedia sopivaan formaattiin ja lähettää se erityyppiseen verkkoon. Mediayhdyskäytävä toimii yhdyskäytävänä eri verkkojen välillä ja esimerkiksi mediayhdyskäytävällä voi muuttaa IP-puhelun piirikytkentäiseen puhelinverkkoon sopivaksi. Mediayhdyskäytävät voidaan jakaa eri luokkiin niiden tarkoituksen mukaisesti. Pienet mediayhdyskäytävät voivat olla ATA-sovittimia, joihin voidaan kytkeä muutama analoginen puhelin. ATA-sovittimet mahdollistavat analogisten puhelinten tai FAX-laitteiden asentamisen VoIP-verkkoon. Muita pieniä mediayhdyskäytäviä ovat yksittäiset PCI-väylään asennettavat kortit ja GSM-päätelaitteet. Isommat mediayhdyskäytävät ovat liitännäkorteilla täytettäviä hyllyjä, jotka voidaan täyttää tarpeiden mukaiseksi kokonaisuudeksi. [7, s. 75 – 76.] Tässä työssä mediayhdyskäytävänä käytettiin Cisco Systems 186 ATA-sovitinta.

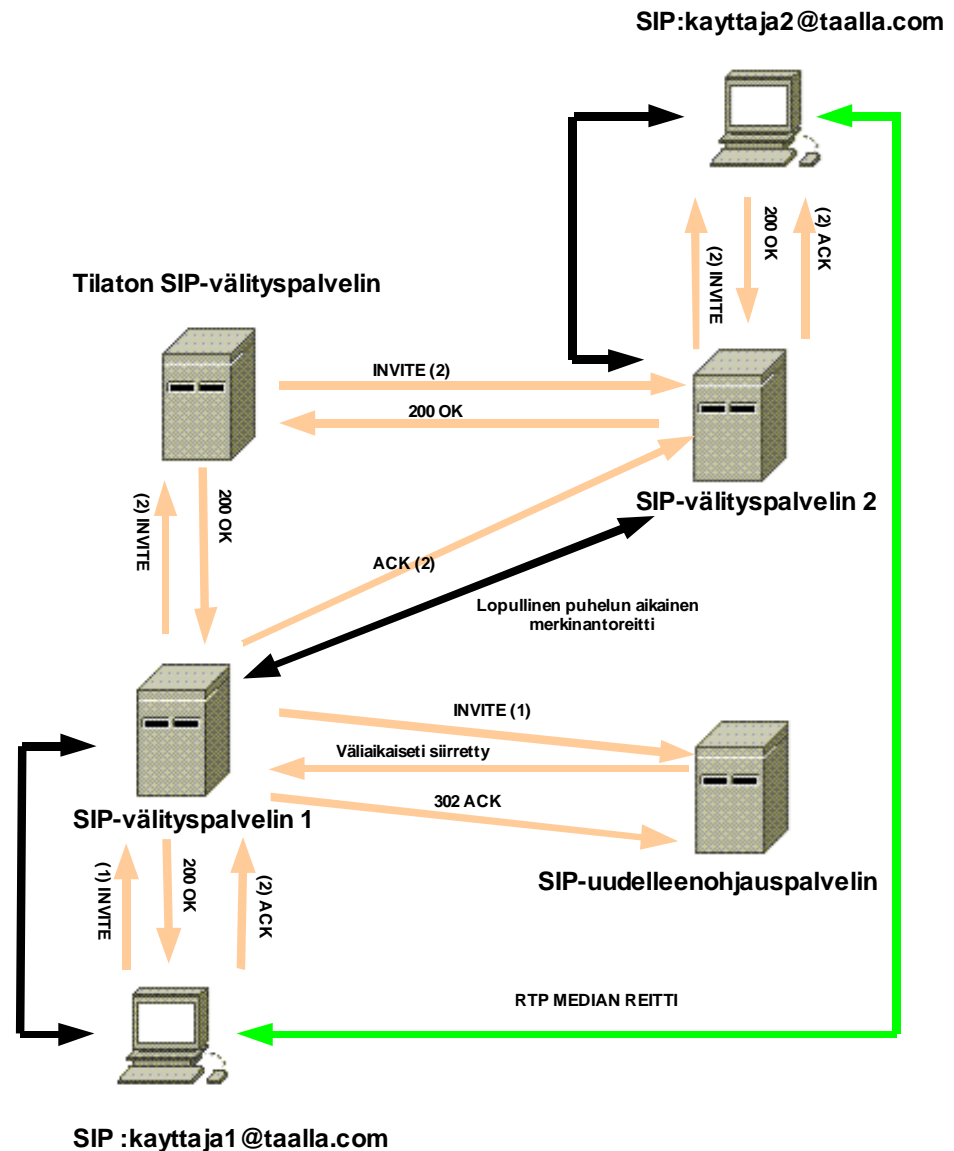
### 3.2. SIP

SIP on IP-pohjaisessa dataverkossa käytettävä merkinantoprotokolla, jolla voidaan muodostaa, purkaa ja hallita päätelaitteiden välisiä istuntoja. SIP on Internet-protokollien standardoinnista vastaavan IETF:n kehittämä. SIP on standardoitu RFC 3261-3264:n mukaisesti, ja se käyttää TCP- ja UDP-porttia 5060 sekä TLS salattuna TCP- ja UDP-porttia 5061. SIP on OSI-mallin sovelluskerroksen tekstipohjainen protokolla, joka toimii OSI-mallin kuljetuskerroksessa UDP- tai TCP-protokollan päällä. VoIP-puhelinjärjestelmän merkinantoprotokollana SIP on yksinkertainen ja soveltuu Internet-liikenteeseen. SIP ja ITU-T:n standardoima H.323 ovat kaksi suosituinta merkinantoprotokollaa. H.323 on edelleen suosittu merkinantoprotokolla, mutta uudemmat järjestelmät ja palvelut käyttävät usein SIP-merkiantoa, koska se soveltuu paremmin dataverkon liikenteeseen. [8, s. 188 – 189.]

SIP-merkinannolla on viisi perustoimintoa: multimediaistunnon muodostamiseen ja purkamiseen. Perustoiminnot ovat käyttäjäpaikannus, käyttäjän käytettävyyden, käyttäjän ominaisuudet, yhteyden asennus ja yhteyden ylläpito. Käyttäjän paikannus tarkoittaa päätelaitteen paikantamista verkossa, jolla

selvitetään, missä haluttu käyttäjä sijaitsee. Käyttäjän käytettävyydellä määritellään, onko käyttäjä vapaana vai varattu. Käyttäjän ominaisuudet toiminto määrittelevät istunnossa käytettävät mediaan liittyvät optiot, kuten puheen koodaukseen käytettävän koodekin. Yhteyden asennus määrittelee muodostettavan istunnon kummankin osapuolen parametrit käyttäen SDP-protokollaa. Yhteyden ylläpito sisältää soitonsiirto-ominaisuuksia, palveluiden käyttöönottoa ja yhteyden purkamisen. [8, s.190; 4, s. 268.]

SIP-standardin mukaan SIP-verkossa on neljä komponenttia. Komponentit ovat käyttäjäagentti, rekisterinpitäjä, välityspalvelin ja uudelleenohjauspalvelin, joista kolme viimeistä ovat usein integroitu yhteen palvelimeen. Käyttäjäagentti on SIP-verkon päätelaite, kuten IP-puhelin, mutta myös mediayhdyskäytävät lasketaan käyttäjäagenteiksi. Rekisterinpitäjä on palvelin, joka pitää kirjaa verkon käyttäjien sijainnista. Välityspalvelin ohjaa SIP-viestejä verkon päätepisteiden välillä, ja uudelleenohjauspalvelin lähettää vastausviestejä, jotka sisältävät seuraavan uudelleenohjauspalvelimen osoitteen tai sijainnin verkossa. [7, s. 190 – 191; 4, s. 268 – 269.]



Kuva 8. SIP-verkko ja sen toiminta.

Kuvassa 8 käyttaja1 pyrkii muodostamaan istuntoa käyttaja2:n kanssa, Istunnon muodostuminen alkaa, kun käyttaja1 lähettää INVITE-viestin välityspalvelin 1:lle, joka välittää INVITE-viestin uudelleenohjauspalvelimelle, joka vuorostaan ilmoittaa, että käyttaja2 on siirretty muualle. Välityspalvelin 1 vastaa siirtoviestiin 302 ACK-viestillä ja lähettää uuden INVITE-viestin tilattomalle välityspalvelimelle, joka vuorostaan toistaa viestin välityspalvelin 2:lle. Välityspalvelin 2 tuntee käyttaja2:n ja lähettää saamansa INVITE-viestin hänelle. Tähän käyttaja2 vastaa OK-viestillä, joka kulkee välityspalvelin 2:lle, tilattoman välityspalvelimen ja välityspalvelin 2 kautta käyttaja1:lle. Tähän käyttaja1 vastaa ACK-viestillä, joka tällä kertaa kulkee lyhyintä reittiä käyttaja2:lle. Istunnon aikana viestit kulkevat mustien nuolien näyttämää reit-

tiä, ja RTP-paketeista koostuva mediavirta kulkee täysin omaa reittiä käyttäjä1 ja käyttäjä2 välillä. Alla on esimerkki SIP INVITE-viestistä, joka kaapattiin talteen GSM-päätelaitteen testauksen yhteydessä.

```
INVITE sip:00505247759@80.221.63.205 SIP/2.0
Via: SIP/2.0/UDP 80.221.54.142:52934;branch=z9hG4bK-d8754z-
2225160ecf5fda58-1---d8754z-;rport
Max-Forwards: 70
Contact: <sip:300@80.221.54.142:52934>
To: "00505247759 (Softphone)"<sip:00505247759@80.221.63.205>
From: "mikko"<sip:300@80.221.63.205>;tag=581c3223
Call-ID: OTJmZjUzNzEyM2FIYjdkOWJmMTBjY2FIQGQ2YmIxNGY.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY,
MESSAGE, SUBSCRIBE, INFO
Content-Type: application/sdp
User-Agent: X-Lite release 1103k stamp 53621
Content-Length: 265
```

```
v=0
o=- 2 2 IN IP4 80.221.54.142
s=CounterPath X-Lite 3.0
c=IN IP4 80.221.54.142
t=0 0
m=audio 3632 RTP/AVP 107 0 8 101
a=alt:1 1 : +WaShaO2 yMPNxvF8 80.221.54.142 3632
a=fmtp:101 0-15
a=rtpmap:107 BV32/16000
a=rtpmap:101 telephone-event/8000
a=sendrecv
```

SIP-viestejä on useita, ja ne ovat selväkielistä tekstiä, joten pakettikaappauksista on helppo selvittää, mitä laitteiden välillä tapahtuu. Viesteistä olennaisimpia ovat viestipyynnöt kuten seuraavat:

- REGISTER, eli puhelimen tai käyttäjän palvelimelle kirjautumiseen käytetty viesti.
- INVITE, eli puhelun tai SIP-yhteyden alullepanoviesti.
- BYE, eli komento, jolla puhelu tai SIP-yhteys katkaistaan.
- CANCEL, eli keskeneräisen istunnon tai puhelun perumiseen käytetty komento.
- ACK, eli puheluun tai yhteyteen liittyvän toiminnon myöntämiseen käytetty viesti.

SIP-protokolla lähettää viesteihin vastauksia, jotka on jaettu vastauskoodisarjoihin, joiden avulla määritellään yhteyden tila. Vastauskoodien tuntemi-

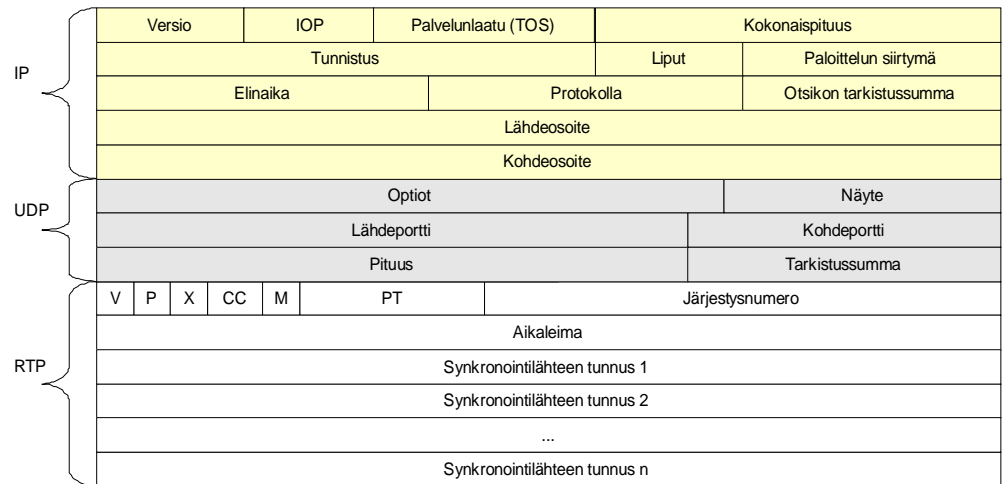


sesta on hyötyä vikatilanteessa, koska niiden avulla voidaan selvittää, missä laitteessa ja mistä syystä vika on syntynyt. 100-sarjan vastaukset viittaavat siihen, että niitä seuraa toinen vastaus. Tämän tyyppisiä vastauksia ovat esimerkiksi: yritetään, hälytetään ja puhelu uudelleenohjataan. 200-sarjan vastauksilla ilmoitetaan, että pyydetty toiminto onnistui. 300-sarja sisältää ohjauksiin viittaavia vastauksia, joita on useita, mutta suurin osa niistä viittaa istunnon tietojen olevan puutteellisia tai vääriä. 400-sarja sisältää asiakaslaitteen virheeseen viittaavat vastaukset. 500-sarjan palvelimen virheeseen viittaavat vastaukset ja 600-sarjan globaalit virheet. [4, s. 272 – 275; 8, s. 191 – 194.] Lista eri SIP-vastauksista ja niiden tarkoitus löytyy liitteestä 1.

### 3.3. Median siirto

Dataverkossa kaikki media on aina aikakriittistä liikennettä, jonka siirrossa tapahtuva viive tulee minimoida ja siirrettävä media tulee olla oikeaan aikaan vastaanottavassa päätepisteessä, koska siitä on hyötyä vain tietyllä hetkellä. Tästä syystä aikakriittiseen liikenteeseen usein suhtaudutaan eri tavalla kuin muuhun dataverkossa kulkevaan liikenteeseen. Medialle annetaan etuoikeus kulkea verkossa. Ruuhkatilanteessa paketteja joudutaan usein pudottamaan, jotta mediaa sisältävät paketit saataisiin siirrettyä kunnolla vastaanottavalle osapuolelle. Puhemedian siirtoon TCP/IP-verkossa käytetään RTP- ja RTCP-protokollia. RTP siirtää reaaliajassa puhepaketteja ja RTCP raportoii verkon toimivuuden tasosta ja lähettää siihen liittyvää mittaustietoa.

IETF standardoi RTP-protokollan RFC 3550:ssa, jonka mukaan RTP käyttää parillisia TCP/UDP-portteja ja RTCP aina näitä seuraavia parittomia portteja, mutta niille on myös rekisteröity käyttöön UDP/TCP-portit 5004 ja 5005. Uusi UDP/TCP-portti otetaan aina dynaamisesti käyttöön tarpeen mukaan, joka tuottaa ongelmia palomuurien kanssa. Tyypillisesti yksi RTP-paketti sisältää 20-40 ms pituisen otteen ihmisen puhetta, joten yksi keskustelun puheenvuoro muodostaa suuren määrään RTP-paketteja. RTP-paketin otsikossa on järjestysnumero ja aikaleima, joiden avulla vastaanottava päätelaite pystyy järjestämään paketit oikeaan järjestykseen. Vastaanottava päätelaite puskuroi RTP-paketteja, jotta ne voidaan soittaa putkeen aikamerkkauksen mukaisessa järjestyksessä. Puskuroinnin avulla peitetään medianvirran viivettä ja viiveen vaihtelua, joka syntyy kun paketit siirretään verkon yli käyttäjältä toiselle. [7, s. 174-177] Kuvassa 9 on esitetty RTP-paketti OSI-mallin verkkokerroksen IP-otsikkoon ja kuljetuskerroksen UDP-otsikkoon sidottuna.



Kuva 9. RTP/UDP/IP-paketti. [4, s. 161.]

Kuvassa 9 esitetyn RTP-otsikon V-kenttä kertoo RTP-protokollan version, P-bitti on täytebitti, X-bitti on sovelluskohtainen laajennusbitti ja CC-kenttä määrittelee lähetävien osapuolien lukumäärän, joita on puheluiden tapauksessa aina yksi. M-bitti on sovellus-kerroksen käyttämä arvo, jolla kerrotaan, että kyseinen paketti sisältää sovelluksen kannalta olennaista dataa. PT-kenttä kertoo paketin datan formaatin, kuten käytettävän koodekin. Järjestysnumeron avulla paketit saadaan vastaanotopäässä järjestettyä lähetysjärjestykseen. Aikaleima ilmaisee, milloin kyseisen paketin sisältämä puhenäyte on otettu. Synkronointilähteen tunniste määrittelee lähetävälle osapuolelle identiteetin. Jokainen RTP-paketteja lähettävä osapuoli saa oman identiteetin, jonka avulla osapuolet voidaan eritellä. CSRC-identiteetti määrittelee listan lähetävistä osapuolista, jonka avulla eri mediavirrat voidaan tarvittaessa yhdistää. [8, s. 177 – 181.]

RTCP on määritelty samassa standardissa kuin RTP, mutta IETF näki RTCP:n rajatuksi protokollaksi ja siitä kehitettiin monipuolisempi versio standardissa RFC 3611. RTCP-raportteja sisältäviä RTCP-paketteja lähettävät kaikki yhteyden osapuolet. Raportteja lähetetään yleensä viiden sekunnin välein ja ne kerätään talteen monitorointityökaluihin, jotka voivat olla myös kolmannen osapuolen laitteita. [7, s. 174 – 175, s. 179 – 181.]

RTCP-raporttien päätyypit ovat lähettäjän raportti, joka sisältää lähetys- ja vastaanostotilastitietoa, kuten lähetävän osapuolen lähettämät paketit, kadonneiden paketien lukumäärän, paketien katoamisprosentti ja saapumisvärinän. Kadonneet paketit perustuvat yhteyden vastapuolen lähettämiin lähettäjä raportteihin. Vastaanottajan raportti sisältää vastaavat tilastit, ja

kuin lähettäjä raportti, mutta vastaaja raportti generoidaan vain silloin, kun osapuoli ei ole lähettänyt paketteja edellisen raportin jälkeen. Lähettäjän kuvaus paketti sisältää tietoa lähettävästä osapuolesta ja sen ominaisuuksista. APP-sovelluspaketti on varattu kokeilukäyttöön. [7, s. 179 – 181.]

### 3.4. Inter-Asterisk eXchange

Inter-Asterisk eXchange on Asterisk yhdyskäytävän merkinantoon käytettävä protokolla, jota pääasiassa käytetään yhdistämään Asterisk-palvelimia toisiinsa. IAX on yhdyskäytävän merkinannossa muita merkinantoprotokollia yksinkertaisempi, ja se on suunniteltu läpäisemään palomuurit ja NAT-muunnokset sekä minimoimaan käytettävä kaista. Lisäksi IAX:ää varten palomuuereista tulee avata vain yksi portti ja sitä voidaan käyttää myös päätelaitteiden merkinantoon. IAX:lle on IETF:n epävirallinen määritelmä standardiksi RFC 5456 ja sillä on virallisesti määritelty käyttöön UDP-portti 4569. [7, s. 195.]

IAX eroaa muista merkinantoprotokollista, koska se ei erottele istuntoa kahden vaiheeseen eli istunnon muodostamista, hallintaa ja purkamista sekä median siirtoa. IAX limittää kumpaankin vaiheeseen liittyvät toiminnot yhteen UDP-virtaan, joka selviää NAT-muunnoksista ja palomuuereista huolettomasti. IAX-puhelun kulkiessa usean palvelimen kautta IAX pyrkii ohjaamaan liikenteen kulkemaan vain päätepisteiden välillä, mutta mikäli tämä ei onnistu IAX palaa aikaisempaan toimintamalliin. IAX tukee MD5- ja RSA-varmennusta ja IAX-paketit voidaan salata 128 bitin AES-kryptauksella. [7, s. 195 – 197.] IAX-istuntojen muodostamisperiaate on altis DoS-hyökkäyksille, koska se vastaa ACK-viestillä kaikkiin istunnossa onnistuneisiin toimintoihin. IAX on helppo ottaa käyttöön, joten se soveltuu hyvin kotikäyttöön tai hajautettuun verkkoon.

### 3.5. Palvelun laatu

Palvelun laatu (QoS) voi tarkoittaa montaa eri asiaa, mutta sillä usein viitataan tekniikoihin, joiden avulla dataverkossa voidaan sovelluskohtaisesti hankkia kaistanleveyttä ja vähentää viivettä. QoS:n avulla pyritään vähentämään verkon pakettien hävikkiä, paketeissa tapahtuvia bittivirheitä, pakettien saapumista epäjärjestyksessä, värinää (jitter) ja latenssia. Latenssilla tarkoitetaan paketin edestakaiseen matkaan kuluvaa aikaa lähettäjän ja vastaanottajan välillä. Värinällä tarkoitetaan paketin latenssin muutosta aikaan näh-

den eli viiveen vaihtelua. ITU-T G. 114 suosituksen mukaan hyvän äänen laadun latenssi tulisi olla enintään 150 ms yhteen suuntaan. [4. s. 171.]

Tässä työssä käytettiin palvelutyyppiin (ToS) perustuvaa QoS-tekniikkaa ja siitä kehitettyä uudempaa Diffserv-tekniikan DS-kenttää (RFC 2474). Näiden tekniikoiden avulla IP-paketit merkataan eri luokkiin, jotta kriittiset IP-paketit voidaan siirtää eteenpäin ennen vähemmän kriittisiä paketteja. Merkkkaus tehdään IP-otsikkoon kolmen bitin ToS-kenttään (kuva 9) tai kahdeksan bitin DS-kenttään, jossa ECN-kenttä vie kaksi bittiä ja DSCP-kenttä kuusi bittiä. ToS-bitit määrittelevät kahdeksan eri palvelutyyppiä ja ne on esitetty DSCP arvojen kanssa taulukossa 1. Osa DS-biteistä vastaa ToS-bittiä, mutta DS-bitit jaetaan luokkiin siedettävän pakettihävikin perusteella. [4, s.169, 180 – 181; 9.]

Palveluluokka (CoS) on ToS-merkkausta vastaava QoS-tekniikka, joka tehdään OSI-mallin siirtokerroksessa. CoS-merkkkaus tehdään ethernet-otsikkoon kolmen bitin CoS-kenttään, mikä voidaan tehdä, kun 802.1Q eli VLAN-merkkkaus on käytössä. CoS-merkkauksen avulla päätelaitteen ja kytkimen sekä kahden kytkimen välillä siirretyt paketit voidaan priorisoida. Tässä työssä ei toteutettu CoS-merkkausta, koska työssä käytetty kytkin ei tukenut 802.1Q:ta.

Taulukko 1. Suositellut QoS-tekniikoiden arvot eri liikennetyypeille. [4, s. 181; 9.]

ToS	DSCP	CoS	QoS	Merkitys	Liikennetyyppi
0	0	0	0	Rutiini	Data
1	AF11 CS1	1	1	Prioriteetti	Keskitasen prioriteetin data
2	AF21 CS2	2	2	Välitön	Korkean prioriteetin data
3	AF31 CS3	3	3	Flash	Merkinanto
4	AF41 CS4	4	4	Korvattu flash	Videomedia
5	EF	5	5	Kriittinen	Puhemedia
6	CS6	6	6	Internet (verkkojen välinen ohjaus)	Varattu (mm. IP- reititysprotokollat)
7		7	7	Verkonohjaus	Varattu (mm. reitityspäivi- tykset)

Taulukossa 1 on esitetty suositeltavat bittiarvot eri QoS-tekniikoille, kun eri liikennetyyppejä aletaan luokitella. Kriittisimpänä liikenteenä pidetään IP-verkon toimintaan vaikuttavaa liikennettä, kuten reititysprotokollien päivitys- ja ylläpitoviestejä, koska mikään muu liikenne ei voi kulkea, jos verkko ei toimi. Tästä syystä QoS-luokat kuusi ja seitsemän on varattu, eikä muuta liikennettä suositella merkittäväksi näihin luokkiin. Tämän työn kannalta olennaisimmat QoS-luokat ovat taulun 1 mukaan viisi ja kolme, sillä puhemediaa muodostuva RTP-virta merkataan luokkaan viisi ja SIP-merkinanto merkataan luokkaan kolme. Tässä työssä toteutettiin merkinannon ja mediansiirron merkkkaus, jonka toteuttaminen Asteriskissa käsitellään Asteriskin konfiguroinnin yhteydessä.

### 3.6. Puheen koodaus

Ihmispuhe on analogista audiosignaalia, joka tulee digitalisoida koodauksella käyttäen tiettyä näytteenottotaajuutta ja askellusta, jotta sitä voidaan siirtää tietoliikennettä käyttäen. Puheen AD-muunnoksesta syntyvä bittijono otetaan talteen ja siirretään verkon yli toiselle osapuolelle. Koodaukseen käytetään koodekkeja, jotka ovat algoritmeja tai sovelluksia, jotka toteuttavat äänen purkamisen ja pakkaamisen. Tässä tulee ottaa huomioon, että ihminen ei pysty kuulemaan kaikkia ääniaaltoja, joten vain puheen käyttämät äänitaajuudet kannattaa kerätä koodaukseen.

Puheen koodauksessa pyritään mahdollisimman tiiviisti pakattuun lopputulokseen, jonka ihminen pystyy ymmärtämään. Tämä johtuu siitä, että tiiviimin pakattu puhe vie vähemmän kaistanleveyttä ja vähentää siirtoon käytettävän verkon kuormaa. [6, s. 138 – 139] Taulukossa 2 on esitetty yleisimpiä ITU-T-suositusten mukaisia VoIP-verkon puhekoodekkeja ja niiden saamat MOS-pisteet. Tässä työssä asennetut puhelimet käyttivät G.711 ulaw-koodekkia, jonka valintaan liittyvät syyt selvitetään GSM-päätelaitteen asennuksen yhteydessä.

Taulukko 2. Puhekoodekit. [4, s. 153 ; 8, s.187.]

Koodekki (ITU-T)	Siirtonopeus (kbit/s)	Puheen hyötykuorma (bittiä, näytteenotto 20 ms)	Ethernet siirtonopeus (kbit/s)	MOS pisteet
G. 711 (PCM)	64	160	87,2	4,1
G. 726 (APCM)	32	80	55,2	3,85
G. 729a	8	20	31,2	3,7

Taulukosta 2 huomaa, miten tehokkaampi koodekki vaatii huomattavasti vähemmän kaistaa yhtä puhelua kohden, mutta puhelun äänenlaatu huononee. Yhden G.711-puhelun kaista riittää melkein kolmeen G.729a koodekin puheluun, kun puhelut kulkevat ethernet-tekniikkaa käyttävässä dataverkossa. MOS-pisteet ovat asteikolla 1 (huono) – 5 (erinomainen) annettuja arvosanoja, jotka kuvaavat koodatun äänen laatua. Tämä on usein koodekkien testauksessa käytetty laadun mittaustesti nimeltään keskivertomielipide. Pistteet ovat kuulijoiden antamista arvosanoista laskettuja keskiarvoja. Taulukon 2 MOS-pisteet on otettu Cisco Labs:n testien tuloksista.

#### 4. ASTERISK

Asterisk on vapaaseen lähdekoodiin perustuva puhepalvelin ohjelmisto, joka on vapaasti käytettävissä GNU GPL lisenssin alaisena. Mark Spencer loi Asteriskin vuonna 1999, jonka jälkeen hän perusti Digium-yrityksen, joka on erikoistunut puhepalvelinten laitteisiin ja ohjelmistoihin. Digium tarjoaa Asteriskin liittyviä ohjelmistoja ja laitteita, joten Digiumin tuotteista voi olla hyötyä yrityksen käyttöön tarkoitetun Asterisk-palvelimen suunnittelussa. Asteriskin nimi tulee \*-merkkiä tarkoittavasta englanninkielisestä sanasta.

Asterisk tukee useita eri käyttöjärjestelmiä kuten Linux, Mac OSX, Windows ja BSD. Linux-käyttöjärjestelmään löytyvät Zaptel-laitteiden ajurit toimivat parhaiten, mutta niitä löytyy myös muille käyttöjärjestelmille. Asterisk on VoIP-puhepalvelin, johon voidaan asentaa myös digitaalisia ja analogisia lankapuhelimia riippuen käytettävistä mediayhdyskäytävistä. Asterisk-puhepalvelin sisältää kaikki puhelinvaihteen perusominaisuudet, tukee yleisimpiä koodekkeja ja käyttää standardoituja protokollia. [7, s. 25 – 27.]

#### 4.1. Vaatimukset

Ohjelmistona Asterisk on hyvin joustava, ja se voidaan asentaa lähes mihin tahansa Linux-ympäristöön, mutta puhepalvelin prosessoi aikakriittisiä puheluita, joita varten sillä tulee olla vapaita resursseja. Asterisk-palvelimena käytettävän tietokoneen laitteistovaatimukset vaihtelevat riippuen puhelinjärjestelmän vaatimuksista. Laitteistovaatimukseen vaikuttaa eniten, kuinka montaa samanaikaista puhelua palvelimen tulee pystyä prosessoimaan. Puheluiden lisäksi laitteistoon vaikuttaa myös numeroanalyysin logiikka, mahdolliset medianmuunnosta tekevät PCI-liitäntään asennetut DSP-kortit, käytettävät koodekit, muut prosessit ja itse käyttöjärjestelmän ytimen toiminta. Suuret Asterisk-järjestelmät ovat hajautettuja järjestelmiä, jotka koostuvat useista palvelimista, jotka voidaan keskittää yhteen tai useampaan prosessointi yksikköön. Taulukossa 3 on esitetty suuntaa antavat laitteistovaatimukset erikokoisille Asterisk palvelinjärjestelmille. [10 s. 11 – 17.]

Taulukko 3. Asterisk-palvelimen laitteistovaatimukset. [10, s. 12]

Tarkoitus	Kanavoiden lukumäärä	Minimi suositus
Harrastus järjestelmä	Enintään 5	400MHz x86, 256MB RAM
Koti/pienikonttori	5 – 10	1GHz x86, 512MB RAM
Pieni yritys	Enintään 25	3GHz x86, 1GB RAM
Pk-yritys (Keski-kokoinen)	Yli 25	Moniydinprosessori, mahdollisesti useista palvelimista rakennettu hajautettu järjestelmä

Työn alkuvaiheessa suunnitteilla oli asentaa Asterisk virtuaalikoneeseen, joka olisi asennettu käytössä olevaan tietokoneeseen, mutta romukupasta löytyi yksi käyttämätön työasema tietokone, joten tämä valittiin Asterisk:n lait-

teistoksi. Tässä työssä palvelimena käytettiin vanhaa työasemaa, jonka laitteisto on esitelty taulukossa 4.

*Taulukko 4. Työssä käytettävän palvelimen laitteisto.*

Proessori	Keskusmuisti	Massamuisti
Intel Pentium 4 CPU 3.06GHz	2x512MHz PC-3200 DDR2-400	40G

Tässä työssä asennetulla palvelimella on 10 - 15 käyttäjää, joista suurin osa ei käytä palvelinta aktiivisesti. Palvelimella on eniten ruuhkaa puhelinkonferenssien aikana, joihin osallistuu arviolta kahdeksan henkilöä, joten palvelimen tulee pystyä prosessoimaan kahdeksaa samanaikaista puhelua. Taulukoita 3 ja 4 verratessa huomataan, että palvelimen laitteisto on tarvittavaa tehokkaampi. Lisäksi siihen ei asenneta DSP-kortteja tai muita mediamuunnosta tekeviä komponentteja, jotka veisivät resursseja. Ylimääräiset resurssit käytetään hyväksi asentamalla muita puhepalvelinsovelluksia samaan palvelimeen.

Palvelimen asennus aloitettiin puhtaalta pöydältä, koska osa komponenteista kerättiin varaosalaatikosta ja asennettiin fyysisesti palvelimeen, joten palvelimen asennus lähti käyttäjärjestelmän asennuksesta. Tässä työssä käytettiin AsteriskNOW-asennuspakettia, jonka mukana tulee Linux CentOS käyttäjärjestelmä.

#### **4.2. AsteriskNOW-asennus**

AsteriskNOW on Digitumin julkaisema helppokäyttöinen ja ilmainen asennuspaketti, joka on tarkoitettu käyttäjille, joilla ei ole kokemusta Linux-käyttäjärjestelmän käytöstä. Tässä työssä asennettu AsteriskNOW-paketti sisältää Linux CentOS 5.3-käyttäjärjestelmän, joka käyttää Linux kernelin versiota 2.6.18, Asterisk-ohjelmiston versiota 1.4.24, FreePBX-ohjelmiston versiota 2.5 sekä kaikki asennuksessa tarvittavat kirjastotiedostot.

AsteriskNOW sisältämä FreePBX-ohjelmisto on www-selaimella toimiva Asteriskin hallintaan tarkoitettu graafinen käyttöliittymä, jonka ansiosta palvelimen hallinta onnistuu ilman Linux-käyttäjärjestelmän tuntemusta. Tässä työssä haluttiin perehtyä Asteriskin toimintaan syvällisemmin, joten FreePBX-ohjelmistoa ei käytetty Asteriskin konfigurointiin. FreePBX:ään saadaan yhteys www-selaimella osoitteesta "http://<Asterisk-palvelimen IP-



osoite >/admin/ ”, jolloin oletuskäyttäjänimi on ”freepbx” ja salasana ”fpbx”. AsteriskNOW-paketti sisältää valmiiksi asennetun Apache HTTP palvelimen, joka kannattaa ottaa pois käytöstä, jos sitä ei tarvita.

AsteriskNOW-paketti löytyy Asterisk-järjestön verkkosivuilta, josta ladattiin AsteriskNOW-levykekuva, joka kirjoitettiin tallennusmedian toimivalle DVD:lle. Palvelintietokoneen BIOS-asetukset muutettiin käynnistymään ensisijaisesti DVD-asemalta, jotta asennus saatiin alkamaan. Asennuksen alkaessa käyttäjä siirtyy ikkunaan, jossa voi tehdä monipuolisempia muutoksia asennukseen. Mikäli muutoksia ei pidetä tarpeellisena, kuten useimmissa tapauksissa, ikkunasta pääsee eteenpäin painamalla <Enter>-painiketta. Itse asennuksessa on kolme askelta.

- Kovalevyjen osiointi. Tässä vaiheessa kaikki tietokoneen kovalevyt jaetaan osioihin. Tässä työssä poistettiin kaikki levyllä oleva vanha data ja kovalevyt osioitiin oletusasetuksilla.
- Aikavyöhykkeen asettaminen. Valitaan oikea aikavyöhyke.
- Pääkäyttäjän(root) salasanan määrittäminen. Määritetään pääkäyttäjän salausna.

Edellä mainittujen kolmen kohdan jälkeen AsteriskNOW-paketti asentaa itsensä automaattisesti. Oletuksena verkkokortti hakee IP-osoitteen DHCP-palvelimelta, joten kirjaututtuaan rootin tunnuksilla sisään järjestelmään voi verkkoasetuksia muuttaa *system-config-network*-komennolla ja *ifconfig*-komennolla näkeä verkkokortin tiedot.

Asterisk voidaan myös helposti asentaa aikaisemmin asennettuun käyttöjärjestelmään. Linux-käyttöjärjestelmissä käyttäen paketinhallintatyökalua, joka vaihtelee riippuen jakeluversiosta. Windows-asennukseen on EXE-asennuspaketti AsteriskWin32.

### 4.3. Hakemistot, tiedostot ja komentotulkki

Asterisk luo asennuksen yhteydessä itselleen kansioita Linuxin tiedostojärjestelmään, joihin se tallentaa eri toimintoihin liittyviä tiedostoja. Ehkä tärkein näistä kansioista on */etc/asterisk/*, joka sisältää kaikki Asteriskin konfiguraatitiedostot Zaptel-laitteiden *zaptel.conf*-tiedostoa lukuun ottamatta. */usr/lib/asterisk/modules/* kansio sisältää kaikki Asteriskin moduulit, eli eri sovellukset, kanavat, formaatit ja koodekit. Oletusasetuksilla Asterisk lataa

kaikki moduulit, mutta ladattavia moduuleita voi muuttaa. `/lib/var/asterisk/` hakemisto sisältää Asteriskin rekisteritietokannat, sekä sen alihakemistoista löytyy Asteriskin käyttämiä tiedostoja kuten RSA-allekirjoitukset sekä kuva- ja äänitiedostoja. `/var/spool/asterisk/` sisältää Asterisk puheluiden ja sovel- lusten valvontatietoa, `/var/run/` sisältää käyttöjärjestelmän prosessien ID:t ja `/var/log/asterisk` sisältää Asterisk:n lokitiedostot. [10, s. 59 – 62.]

Asteriskilla on useita konfiguraatiotiedostoja, joiden lukumäärä riippuu järjes- telmässä olevista toiminnoista, mutta tämän työn kannalta olennaisimpia ovat `sip.conf` ja `extensions.conf`. Pelkästään näitä kahta tiedostoa muok- kaamalla pystyy asentamaan täysin toimivan Asterisk-palvelimen. `Sip.conf` sisältää kaikki SIP-merkinantoa käyttävät laitteet, kuten alaliittymät, kanavat ja mediayhdyskätävät. `Extensions.conf` sisältää Asteriskin numeroanalyys- sin, jossa määritellään puheluiden ohjauslogiikka eli mitä tapahtuu, kun käyt- täjät valitsevat tietyn numeron puhelimestaan.

```
-- Executing [888@default:1] Dial("SIP/300-09e7a330", "SIP/200|60|r") in new
stack
-- Called 200
-- SIP/200-09e7a330 is ringing
-- SIP/200-09e7a330 answered SIP/300-09e7a330
-- Packet2Packet bridging SIP/300-09e7a330 and SIP/200-09e7a330
== Spawn extension (default, 888, 1) exited non-zero on 'SIP/300-09e7a330'
-- Executing [304@default:1] Dial("SIP/300-09e7a330", "SIP/304|60|t") in new stack
-- Called 304*CLI>
-- SIP/304-09e7a330 is ringing
-- SIP/304-09e7a330 answered SIP/300-09e7a330
== Spawn extension (default, 304, 1) exited non-zero on 'SIP/300-09e7a330'
-- Executing [500@default:1] Answer("SIP/300-09e7a330", "") in new stack
-- Executing [500@default:2] MeetMe("SIP/300-09e7a330", "500|cIM") in new stack
== Parsing '/etc/asterisk/meetme.conf': Found
== Parsing '/etc/asterisk/meetme_additional.conf': Found
-- Created MeetMe conference 1023 for conference '500'
-- <SIP/300-09e7a330> Playing 'conf-onlyperson' (language 'en')
== Spawn extension (default, 500, 2) exited non-zero on 'SIP/300-09e7a330'
-- Executing [520@default:1] Wait("SIP/300-09e7a330", "1") in new stack
-- Executing [520@default:2] Playback("SIP/300-09e7a330", "/var/lib/asterisk/sounds/custom/record_viesti") in new stack
-- <SIP/300-09e7a330> Playing '/var/lib/asterisk/sounds/custom/record_viesti' (language 'en')
)
-- Executing [520@default:3] SayDigits("SIP/300-09e7a330", "20") in new stack
-- <SIP/300-09e7a330> Playing 'digits/2' (language 'en')
-- <SIP/300-09e7a330> Playing 'digits/0' (language 'en')
-- Executing [520@default:4] Wait("SIP/300-09e7a330", "2") in new stack
-- Executing [520@default:5] Record("SIP/300-09e7a330", "/tmp/prompt20:wav") in new stack
-- <SIP/300-09e7a330> Playing 'beep' (language 'en')
hoas-fe3fdd00-205*CLI>
```

Kuva 10. Asterisk-komentotulkilla seurataan testipuheluita.

Asterisk-komentotulkkiin pääsee käsiksi `/sbin/asterisk -r` komennolla, joka yhdistää käyttäjän käynnissä olevaan Asterisk-prosessiin tai käynnistää uuden Asterisk-prosessin. Kuvasta 10 huomataan, että komentotulkki on hyödyllinen työkalu puheluiden seuraamisessa. Komentotulkissa on paljon hyö-

dyllisiä toimintoja kuten merkinantokanavien tietojen tulostaminen, häiriöiden etsintä ominaisuuksia, merkinantokanavien tilan seuraaminen ja puheluiden muodostumisen seuraaminen. Kaikkien konfiguraatitiedostoihin tehtävien muutoksien jälkeen Asteriskin moduulit tulee lukea uudelleen järjestelmään komentotulkin komennolla *module reload*, jonka jälkeen uudet konfiguraatit otetaan käyttöön.

## 5. KONFIGUROINTI

Puhelinjärjestelmänä Asterisk on hyvin modulaarinen ja skaalautuva, koska siinä saa toimimaan eri laitevalmistajien laitteita, kuten tässä työssä todettiin. Asteriskin konfigurointi tehdään muuttamalla konfiguraatitiedostojen sisältöä tai komentorivillä annettavilla komennoilla. Asterisk pitää konfiguroida vaiheittain suorittamaan eri puheluiden prosessointiin käytettäviä sovelluksia, joka käytännössä muistuttaa ohjelmointia. Sovellukset suorittavat hyvin pieniä operaatioita, joten yksittäisten puhelimien virittely onnistuu helposti. Tämä on yksi Asteriskin vahvuuksista, mutta samalla heikkous, koska samat asiat voidaan tehdä yksinkertaisesti tai monimutkaisesti.

### 5.1. Numeroanalyysi

Numeroanalyysi (Dialplan) on puhelinjärjestelmien käyttämä logiikka, joka määrittelee, miten puhelut prosessoidaan ja ohjataan. Käytännössä tämä tarkoittaa sitä, että numeroanalyysissä määritellään mitä tapahtuu soittaessa tiettyyn ulkoiseen tai sisäiseen puhelinnumeroon. Numeroanalyysin numerointia tulee suunnitella ja miettiä etukäteen, jotta järjestelmän numerokapasiteetti riittää kaikille nykyisille ja tuleville alaliittymille, yhdyskäytävillä ja palveluille. Numerointi kannattaa suunnitella loogiseksi, koska se helpottaa järjestelmän hallintaa. Numeroavaruus voidaan jakaa esimerkiksi maantieteellisen sijainnin, toimipisteen tai paikkakunnan mukaan. Tämän lisäksi osa numeroavaruudesta kannattaa varata lyhytvalinnoille, ACD-sarjoille ja ACD-agentteille. Tässä työssä käytettiin taulukon 5 mukaista numerointia.

Taulukko 5. Työssä käytetty numerointi.

Tarkoitus	Numeroalue
Sisäiset ohjaukset, hätänumero	1xx
Yhdyskäytävät, sisään tuleva liikenne	2xx
Erikoistapaukset ja testipuhelimet	3xx
Käyttäjien alaliittymät	4xx
Konferenssit, sarjat, viestien äänitys	5xx
Varattu (tulevat alaliittymät)	6xx
Varattu (tulevat alaliittymät)	7xx
Lyhytvalinnat	8xx
Välittäjä	9xx

Asteriskin numeroanalyysi määritellään `extensions.conf`-tiedostossa, joka jaetaan asiayhteyksien mukaan osiin. Operaatiot alkavat aina komennolla `'exten =>'`. Numeroanalyysin syntaksi on:

```
exten => nimi,prioriteetti,komento(parametrit)
```

Nimi viittaa alaliittymälle annettuun asiayhteyteen, kuten käyttäjänimeen tai puhelinnumeroon, prioriteetti kertoo, missä järjestyksessä komennot tulee suorittaa ja `komento()` kohtaan annetaan suoritetta Asterisk komento ja sen parametrit. Komennot voivat olla myös itse kirjoitettuja makroja, joiden avulla numeroanalyysin muokkaamista voidaan helpottaa.

```
exten => _400,1,Dial(SIP/400,60,t)
```

```
exten => _400,n,Playback(vm-nobodyavail)
```

```
exten => _400,n,Hangup
```

*Esimerkki 1. SIP-alaliittymän ohjaukset numeroanalyysissä.*

Esimerkissä 1 on tavanomainen ohjaus SIP-alaliittymälle. Valitessa alanumero 400 käytetään ensin `Dial`-komentoa, joka hälyttää SIP-alaliittymää 400 seuraavat 60 sekuntia, jos alaliittymä ei vastaa puheluun soitetaan `vm-nobodyavail` ääniviesti, jonka jälkeen puhelu puretaan.

Numeroanalyysin määritellään usein oletusasetuksia varten oma asiayhteys, kuten esimerkissä 2 `general-asiayhteys`. Esimerkissä 3 `autofallthrough=yes` rivillä sallitaan puheluiden putoaminen numeroanalyysistä. Tällä estetään puheluiden jumittuminen numeroanalyysin tietyille riville, mikäli suoritettava

sovellus ei toimi oikein. Rivi *clearglobalvars=no* vuorostaan kertoo, että muissa konfiguraatitiedostoissa asetettuja globaaleja muuttujia ei putsata.

*[general]*

*autofallthrough=yes ; Sallitaan puhelun putoaminen numeroanalyysistä.*

*clearglobalvars=no*

*[globals]*

*CONSOLE=Console/dsp*

*EXT300=SIP/300*

*EXT301=SIP/301*

*EXT302=SIP/302*

*EXT303=SIP/303*

*EXT304=SIP/304*

*Esimerkki 2. Oletusasetukset ja globaalit muuttujat.*

Numeroanalyysiin voidaan myös määritellä globaaleja muuttujia, joita voidaan käyttää hyväksi makroissa ja numeroanalyysin yksinkertaistamisessa. Esimerkissä 2 EXT300 globaali muuttuja saa arvokseen SIP-alaliittymän 300, joten numeroanalyysissä voidaan viitata SIP-alaliittymään 300 SIP/300 sijaan merkkijonolla EXT300.

## 5.2. SIP-kanavat

Asteriskin kannalta kaikki merkinantoa käyttävät laitteet ovat kanavia riippumatta siitä, onko kyseessä puhelin, yhdyskäytävä vai mediayhdyskäytävä. Kanavat on jaettu kolmeen eri ryhmään: peer-, user- ja friend-kanaviin. User-kanavaa käytetään, kun tarkoituksena on ohjata puheluita palvelimelle. Peer-kanavaa käytetään, kun halutaan soittaa puheluita palvelimelta. Friend-kanavaa vuorostaan käytetään, kun molemmat tilanteet ovat käytössä. Puhelimet käyttävät yleensä friend-kanavaa, mutta esimerkiksi toinen Asterisk-palvelin, jossa on käytössä tietty osa numeroalueesta asennetaan Peer-kanavaksi, koska kaikki kyseisen numeroalueen puhelut lähetetään tähän kanavaan. [11, s. 87.]

Kaikki tässä työssä käytetyt laitteet konfiguroitiin käyttämään SIP-merkinantoa, joten niiden konfiguroinnit tehtiin sip.conf-tiedostoon, joka sijaitsee */etc/asterisk-*kansiossa. IAX-merkinantoa käyttävien kanavoiden konfigurointi toteutetaan hyvin samankaltaisesti kuin SIP-kanavien, joten kun

osaa konfiguroida SIP-kanavia, osaa konfiguroida IAX-kanavia. Sip.conf-tiedoston sisältö voidaan jakaa kahteen osaan: oletusasetuksiin ja kanava-kohtaisiin asetuksiin. Esimerkissä 3 on oletusasetuksien määrittely esimerkki ja selostukset asetusten merkityksestä.

*[general]*

*context=default*

*allowguest=yes ; Sallitaanko anonyymit puhelimet Asterisk.*

*disallow=all ; Kielletään kaikki koodekit, jotta voidaan sallia käytetyt.*

*allow=ulaw ; Määritellään käytettävä koodekki*

*dtmfmode=rfc2833 ;Määritellään DFTM-asetukset*

*canreinvite=no ; Sallitaanko istunnon muodostumisen jälkeen reINVITE-viestien lähetys. Tämä kannattaa aina kieltää, koska päätelaitteiden ohjelmistossa voi olla ohjelmointivirheitä, mutta pitää sallia, jos päätelaite on NAT-muunnoksen tai palomuurin takana.*

*tos\_sip=cs3 ;Määritellään merkinantoliikenteen DSCP-arvo*

*tos\_audio=ef ;Puhe RTP-virran pakettien DSCP-arvo*

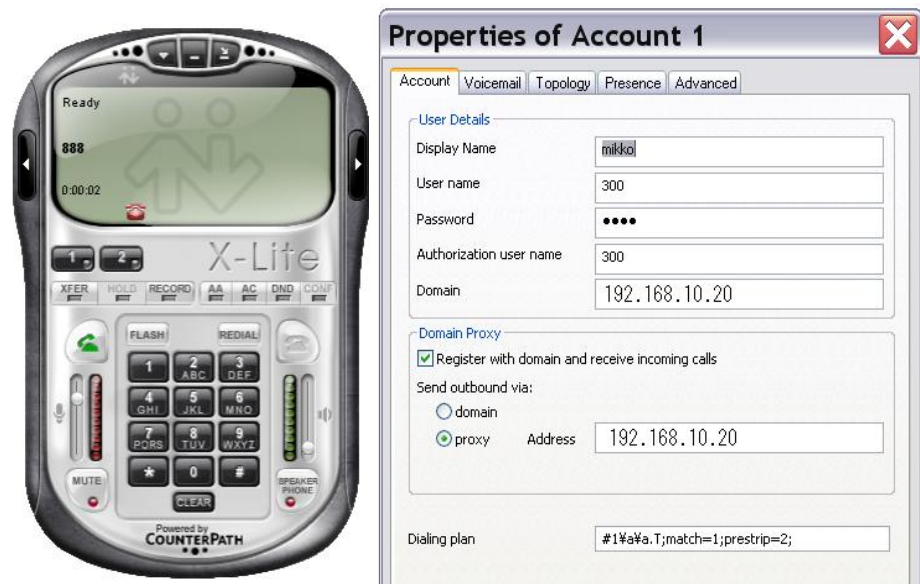
*tos\_video=af41 ;Video RTP-virran pakettien DSCP-arvo*

*language=fi ;Käytetyt maakohtaiset äänitaajuudet*

*Esimerkki 3. SIP-kanavien oletusasetukset.*

### *SIP-ohjelmistopuhelin*

Suurin osa tässä työssä asennetuista päätelaitteista oli SIP-merkinantoa käyttäviä ohjelmistopuhelimia. Käytettäväksi ohjelmistopuhelimeksi valittiin X-lite, joka on ilmainen CounterPath yrityksen kehittämä ohjelmisto. X-lite on kehitetty Windows-, Linux- ja MAC-käyttöjärjestelmille oma versio ja sen graafinen käyttöliittymä on luonnollisen näköinen. Kuvassa 11 on esitelty X-lite-ohjelmistopuhelimen käyttöliittymä ja sen SIP-tilin asetukset.



Kuva 11. X-lite-ohjelmistopuhelin ja SIP-käyttäjätilin asetukset.

Alla on selostettu X-lite-ohjelmistopuhelimen asetukset ja mitä niihin tulee laittaa.

- Display name – Soittaessa näytettävä soittaja ID. Tähän voidaan laittaa esimerkiksi käyttäjän nimi.
- User Name – Käyttäjänimi, jolla puhelin kirjautuu puhepalvelimelle. Käyttäjänimi on käytössä olevan kanavan nimi eli tässä työssä puhelimen numero.
- Password – Salasana, jolla puhelin kirjautuu puhepalvelimelle.
- Authentication username – Oikeaksi vahvistuksessa käytettävä käyttäjänimi. Tämän arvo riippuu käytettävästä vahvistuksesta esimerkiksi käyttäjänimi.
- Domain – Verkkoalue eli puhepalvelimen IP-osoite tai DNS-nimi.
- Send outbound via ->Proxy - Address – Uudelleenohjauspalvelimen eli Asterisk-palvelimen IP-osoite tai DNS-nimi.

Esimerkissä 4 on esitelty tavallisen SIP-ohjelmistopuhelimen konfiguraatiot sip.conf-tiedostossa.

*[410] ; SIP-kanavan nimi, tässä tapauksessa alanimero  
 type=friend ; Liittymän tyyppi  
 context=default ; Asiayhteys  
 callerid="Joulupukki" ; CallerID, eli soitettaessa näytettävä nimi  
 allow=ulaw ; G. 711 PCM ulaw koodekki käytössä*

*host=dynamic ; Alaliittymän sitominen IP-osoitteen. Dynamic-parametri ei sido alaliittymää IP-osoitteeseen.*

*Username=410 ; Alaliittymän käyttäjänimi*

*password=410 ; Alaliittymän salasana*

*Esimerkki 4. SIP-ohjelmistopuhelimen konfiguraatiot.*

#### *IP-puhelin*

Yhdelle puhepalvelimen käyttäjälle asennettiin kotiin tavallinen IP-puhelin. Asennettu IP-puhelin oli Ericsson (nykyään Astran) valmistama Dialogi 4422 mallin (kuva 12) pieni toimistokäyttöön tarkoitettu IP-puhelin. Oletusasetuksilla Dialog 4422 käyttää merkinantoon H.323-protokollaa, mutta sen voi konfiguroida käyttämään SIP-merkinanto. Merkinanto vaihdettiin IP-puhelimen konfiguraatitiedostossa, jonka IP-puhelin haki HTTP-palvelimelta. Dialog 4422-puhelimen konfiguraatitiedosto löytyy liitteestä 2.



*Kuva 12. Ericsson Dialog 4422 IP-puhelin.*

Ericsson Dialog 4422-puhelinta varten Asterisk:n konfiguroitiin hieman erikoinen SIP-kanava. Esimerkissä 5 käytetyt konfiguraatiot ovat kummallisia siksi, että Peer-tyyppisen kanavan tulisi pystyä vain soittamaan puheluita, mutta ei vastaanottamaan niitä. Työssä huomattiin, että Dialog 4422 ei toimi



kunnolla friend-tyyppisenä kanavana, koska se ei pystynyt soittamaan puheluita, mutta pystyi vastaanottamaan niitä. Wireshark-ohjelmalla tehdyistä pakettikaappauksista huomattiin, että merkinanto loppuu SIP-vastaukseen 407 (liite 1), joten Dialog 4422 ei pysty todentamaan välityspalvelimena toimivaa Asterisk-palvelinta.

*[301]*

*type=peer ;Kanavan tyyppi*

*qualify=yes ; Kanavan seuranta. Asterisk seuraa kanavan tilaa*

*context=default*

*callerid="Dialog 4422 IP"*

*host=dynamic*

*allow=ulaw*

*allow=alaw*

*username=301*

*secret=301*

*regexten=301*

*insecure=invite ;Invite-viestiejä ei todenneta*

*Esimerkki 5. Ericsson Dialog 4422 IP-puhelimen konfiguroinnit.*

Esimerkissä 5 löytyy rivi *insecure=invite*, joka muuttaa Asteriskin toimintaa siten, että SIP INVITE-viestejä ei enää tarvitse todentaa, joten tällä päästiin eroon todentamisesta tulevista ongelmista. Todentamisen poistamisesta huolimatta Dialog 4422 ei toiminut friend-kanavana, joten Dialog 4422 toimii eri tavalla kuin tavallinen IP-puhelimen, sillä peer-kanavana se toimi moitteetta.

### 5.3. ATA-sovitin

ATA-sovittimet ovat laitteita, jotka muuttavat IP-paketteina siirrettävän puheen analogiseksi signaaliksi, joten sillä saadaan fakseja tai analogisia puhelimia yhdistettyä VoIP-verkkoon. Halvin tapa asentaa kotiin IP-puhelin on kytkeä vanha analoginen puhelin ATA-sovittimeen. ATA-sovittimessa on yleensä ainakin yksi RJ-11 liittimen FXS-portti ja yksi RJ-45 liittimen verkkoportin portti. Monipuolisemmissa ATA-sovittimissa voi olla FXO-portteja, ADSL-modeemin, IP-reitittimen tai WLAN-reitittimen ominaisuuksia.



*Kuva 13. Cisco Systems ATA 186 puhelinsovitin.*

Tässä työssä asennettiin Cisco Systems 186 ATA-sovitin (kuva 13), jota käytetään yhdyskäytävänä matkapuhelinverkkoon ja analogisen puhelimen sovitinena VoIP-verkkoon. Kuten kuvasta 13 näkee Cisco Systems 186 ATA-sovittimessa on kaksi FSX-porttia ja yksi 10baseT ethernet-portti. Yhteys matkapuhelinverkkoon toteutettiin Nokia 22 PBX GSM päätelaitteen avulla ja analogisena puhelimenä käytettiin Ericsson TEL25-puhelinta, joka on esitetty kuvassa 14. Cisco 186 ATA-sovitin tukee H.323-, SIP-, SCCP-merkinantoprotokollia ja se konfiguroitiin käyttämään SIP-merkinantoa.



*Kuva 14. Analoginen puhelin mallia Ericsson TEL25.*

ATA-sovitinta voi konfiguroida antamalla numerokoodeja DTFM-puhelimesta, käyttäen WWW-selainta tai TFTP-palvelimelta haettavan konfiguraatiodoston avulla. WWW-selaimella konfigurointia varten ATA-sovitin pitää alustaa käyttäen DTMF-puhelinta, joka kytkettiin phone1-porttiin (kuva 13). Liitteessä 3 on ohje, miten ATA-sovittimen alku konfigurointi tulee tehdä.

Ennen WWW-selaimella konfiguroinnin poistoa ATA-sovittimen asetukset otettiin talteen ja lisättiin liitteeseen 3. Jokaista ATA-sovittimeen asennettua puhelinta varten Asteriskin tulee lisätä SIP-kanava. SIP-kanavien konfiguraatiot eivät eroa tavallisista IP-puhelimista tai ohjelmistopuhelimista, mutta huomioitavaa on, että kaikki ATA-sovittimeen asennetut analogiset laitteet jakavat saman IP-osoitteen. ATA-sovittimesta voi seurata puheluiden ja siirrettyyn dataan liittyvää статистиikkaa osoitteesta "http://<ATA-laitteen IP-osoite>/stats".

#### **5.4. AGI- ja AMI-rajapinnat**

Asteriskin skaalautuvaisuus ja monipuolisuus tulee esiin vasta AGI- ja AMI-rajapintojen yhteydessä. Näillä rajapinnoilla Asterisk-ohjelmistoa pystytään

hallitsemaan ulkoisten sovellusten avulla. AGI-skriptien avulla Asterisk voi kommunikoida ulkoisten tietokantojen kanssa ja esimerkiksi numeroanalyysi voidaan antaa kokonaan ulkoisen sovelluksen hallittavaksi. Yleisimpiä ohjelmointikieliä AGI-skriptien toteuttamiseen ovat Perl, Python ja PHP. [10, s. 207 – 208.]

AMI vuorostaan on ohjelmarajapinta, jonka avulla ulkoiset sovellukset voivat hallita ja valvoa Asteriskin toimintaa. AMI-rajapintoja yleensä käytetään Asteriskin integrointiin olemassa oleviin palvelimiin ja järjestelmiin. [10, s. 227 – 228] AGI- ja AMI-rajapinnat ovat tarkoitettu suurempiin ja monipuolisempiin Asterisk puhelinjärjestelmiin, joita on keskisuurin ja suurien yritysten käytössä, joten kotikäytössä ne eivät ole hyödyllisiä.

## 5.5. Puhekonferenssi ja puheposti

Tässä työssä konfiguroitiin muutama puhelinkonferenssi ja käyttäjä kohtaiset puhepostit. Puhelinkonferenssi on palvelu, jossa useampi käyttäjä voi osallistua puhelinkeskusteluun samaan aikaan liittymällä konferenssi siltaan. Asterisk sisältää MeetMe-puhelinkonferenssi sovelluksen, jolla on helppo toteuttaa puhelinkonferenssi siltoja. Meetme-puhelinkonferenssi konfiguroidaan esimerkin 6 mukaisesti numeroanalyysiin ja meetme.conf-tiedostoihin.

```
##### extensions.conf tiedostossa #####;
```

```
exten => _500,1,Answer()
```

```
exten => _500,n,MeetMe(500,c,IM) ;Konferenssi numero 500, optiot c,I ja M
```

```
exten => _500,n,Hangup()
```

```
##### meetme.conf tiedostossa #####;
```

```
conf => 500,1234,12345 ;Konferenssinumero 500, pin-koodi 1234,  
hallinto pin-koodi 12345
```

*Esimerkki 6. Puhelinkonferenssi.*

Esimerkissä 6 esitettyssä puhelinkonferenssissa on käytössä muutama lisätoiminto, jotka saadaan optioilla c, I ja M käyttöön. c-optiolla ilmoitetaan konferenssin jäsenien lukumäärän liittyessä konferenssiin, I-optiolla ilmoitetaan aina, kun konferenssin jäsen poistuu konferenssista ja M-optiolla konferenssissa soi jonotusmusiikki, jos konferenssissa on vain yksi henkilö. Meetme.conf-tiedoston konfiguroinnissa PIN-koodilla kirjaututaan konferenssiin sisään ja hallinta PIN-koodilla voi kirjautua konferenssin ylläpitäjäksi.

Puheposti on yksi yleisimmistä puhelinpalveluista, joka tunnetaan usein paremmin nimellä vastaaja. Puhepostin tarkoituksena on saada käyttäjät paremmin tavoitettavaksi heille soittaville henkilöille. Puhepostin ideana on se, että kun käyttäjä ei vastaa hänelle tulevaan puheluun tiettyyn aika raajaan mennessä, siirtyy puhelu puhepostiin, jossa soittaja voi jättää ääniviestin.

```
;### voicemail.conf ###;
```

```
302 => 1234,Aapeli Asentaja,Aapo@jokudomain.com,tld
```

```
;### extensions.conf ###;
```

```
exten => _302,1,Dial(SIP/302,60,t)
```

```
exten => _302,n,GotoIf("${DIALSTATUS}" = "BUSY")?busy:unavail)
```

```
exten => _302,n(unavail),Voicemail(302@default,u)
```

```
exten => _302,n,Hangup
```

```
exten => _302,n(busy),VoiceMail(302@default,b)
```

```
exten => _302,n,Hangup
```

```
exten => _1400,1,VoiceMailMain()
```

*Esimerkki 7. Puheposti.*

Esimerkissä 7 esitellyssä puheposti konfiguroinneissa voicemail.conf-tiedostoon luodaan alaliittymällä 302 puhepostilaatikko, jonka salasana on 1234, postilaatikon omistaja on Aapeli Asentaja ja saapuvista puheposteista lähetetään ilmoitus sähköpostitse osoitteeseen Aapo@jokudomain.com. Alaliittymälle 302 ohjelmoitiin puheposti käyttöön, siten että alaliittymälle tulvat puhelut ohjautuvat puhepostiin, jos alaliittymän tila on varattu tai ei tavoitettavissa. Kaikki käyttäjät voivat kuunnella omia puhepostejaan valitsemalla numeron 1400, jonka jälkeen heidän tulee antaa puhepostilaatikon numero ja salasana.

## 6. GSM-PÄÄTELAITE

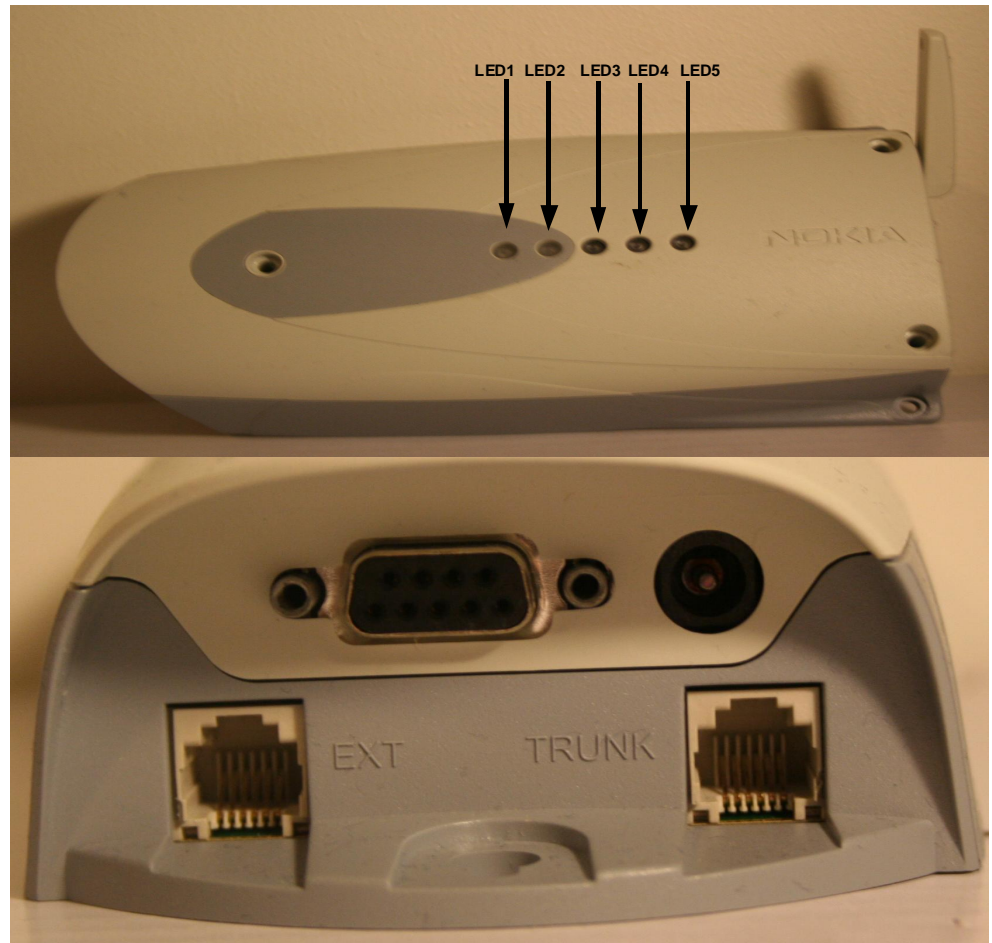
Asterisk-puhepalvelin voidaan yhdistää monella eri tavalla julkiseen puhelinverkkoon ja riippuen yhdistys tavasta laitteeseen saadaan lisää ominaisuuksia. Yleensä puhepalvelin liitetään julkiseen puhelinverkkoon käyttäen DSP-kortteja, jotka voidaan asentaa puhepalvelimen PCI-väylään. DSP-kortteja voidaan asentaa myös reitittimiin tai erillisiin mediayhdyskäytävänä toimiviin laitteisiin. Osa suomalaisista telenoperaattoreista tarjoaa myös SIP-merkinannolla toimivaa vaihdeliittymää. Tässä työssä keskitytään Asterisk

puhepalvelimen yhdistämiseen matkapuhelinverkkoon käyttäen GSM-päätelaitetta.

Puhepalvelimen yhdistämiseen julkiseen verkkoon voidaan käyttää GSM-päätelaitteita, jotka olivat 2000-luvun alussa suosittuja, koska lankapuhelimesta soittaminen matkapuhelimeen oli huomattavasti kalliimpaa kuin matkapuhelimesta soittaminen matkapuhelimeen. Puhepalvelimet konfiguroitiin ohjaamaan matkapuhelimiin lähtevät puhelut GSM-päätelaitteiden kautta, niin kauan kuin GSM-päätelaitteiden aikavälejä oli vapaana. GSM-päätelaitteella saadaan käyttöön yksi tai useampi aikaväli riippuen asennettavien SIM-korttien lukumäärästä. Julkisessa puhelinverkossa GSM-päätelaitteella on siihen asennetun SIM-kortin puhelinnumero. GSM-päätelaitteet voidaan konfiguroida ohjaamaan kaikki saapuvat puhelut tiettyyn numeroon tai lähettämään soittajalle valintääntä, jolloin soittaja voi valita numeron johon hän haluaa soittaa. GSM-päätelaitte sopii hyvin kotikäyttöön, koska kotona harvoin tarvitsee vastaanottaa useita puheluita samaan aikaan.

### **6.1. Nokia 22 PBX**

Työssä käytettiin Nokia 22 PBX GSM päätelaitetta, jonka avulla voidaan soittaa puheluita matkapuhelinverkkoon. GSM-päätelaitte toimii kaksoistajuuskaistalla, joten se voidaan yhdistää sekä GSM900, että GSM1800 verkkoon riippuen teleoperaattorista. Laite myös tukee GSM+2-palveluita ja piirikytkentäistä HSCSD-datansiirtoa maksiminopeudella 43,2 kbit/s. [12.]



*Kuva 15. Nokia PBX 22 GSM päätelaite.*

Kuten kuvasta 15 näkee, Nokia PBX 22 GSM-päätelaitteessa on kaksi RJ-11 liittimen puhelinporttia ja yksi DE-9 pin RS-232 -sarjaportti. Puhelinportit EXT-portti ja TRUNK-portti on tarkoitettu puhelinjärjestelmään kytkentää varten. Nokia 22 toimii puhelinjärjestelmän alaliittymänä, kun se on kytkettynä EXT-porttiin. Tässä tapauksessa puhelinjärjestelmästä syötetään jännitettä Nokia 22:lle. TRUNK-porttiin kytkettynä Nokia 22 tulee asentaa puhelinjärjestelmän analogiseen keskusjohtoporttiin, sillä Nokia 22 syöttää tarvittavan jännitteen tässä tapauksessa. TRUNK-porttia käytetään myös Nokia 22 GSM-päätelaitteen konfigurointiin. Lisäksi TRUNK-porttiin voidaan kytkeä analoginen puhelin, joka pystyy soittamaan ja vastaanottamaan puheluita kytkennän jälkeen. Sarjaportti on tarkoitettu SMS-viestien lähetyksiä varten. Sarjaportilla tietokoneeseen kytketty Nokia 22 pystyy lähettämään SMS-viestejä, mikäli sitä komennetaan sarjaportin kautta AT-komentokielellä. Tässä työssä ei toteutettu SMS-viestien lähetyksiä, joka jää tulevaisuuden projektiksi.

GSM-päätelaite tulee asentaa ainakin 20 cm:n päähän käyttäjistä, ja sen asennus on hyvin yksinkertainen. Lisää SIM-kortti laitteen sisään, kytke laitteeseen DTMF-puhelin GSM-päätelaite TRUNK-liitäntään ja anna PIN-koodi ja #-merkki esimerkiksi "1234#". Tämän jälkeen saat valintaäänien puheli-meesi, jonka jälkeen voit tehdä testipuheluita. Taulukossa 6 on esitetty merkkiäänet, joita laite voi lähettää, joista on apua vikatilanteessa. [12]

Taulukko 6. GSM-päätelaitteen antamat merkkiäänet. [12]

Merkkiääni	Merkitys
-----	Asenna SIM-kortti
- _ _ - _ _ - _ _	Anna PIN-koodi
- -	Anna PUK-koodi
- - - -	Virhe
	OK
- - - - - - - -	SMS-viesti saapui

GSM-päätelaitteen tilaa voi tarkkailla päätelaitteen viidestä LED-valosta, jotka ovat nähtävissä kuvassa 15. LED 1 ja LED 2 määrittelevät käytössä olevan toimintatilan, eli toimiiko Nokia 22 yhdyskäytävänä vai alaliittymänä. Taulukon 7 mukaisten valomerkkien avulla voidaan seurata Nokia 22 GSM-päätelaitteen toimintaa.



Taulukko 7. Nokia 22 PBX GSM-päätelaitteen LED-valojen merkitykset. [12]

LED 1	LED 2	LED 3	LED 4	LED 5	Merkitys
Palaa					Yhdyskäytävä-tila.
	Palaa				Alaliittymä-tila.
-	-	-	-	-	Ei sähkövirtaa.
		Välkkyy	-	-	Sähkövirta kytketty. Yhdistetään GSM-verkkoon.
		Palaa	-	-	Laite toiminnassa.
		Palaa	-	Palaa	Puhelu kesken.
		Palaa	Välkkyy	-	Päätelaite vastaanottaa puhelua.
		-	Välkkyy	-	Anna PIN-koodi.
		Välkkyy	Välkkyy		Anna PUK-koodi.
		Palaa	Palaa	Palaa	Päätelaite on vastaanottanut SMS-viestin tai puhepostin.
		Palaa	Palaa	Välkkyy	Päätelaitteen muistissa ei ole tilaa uudelle SMS-viestille, joten vanhin SMS-viesti tuhoetaan.
		-	Välkkyy	Välkkyy	Asenna SIM-kortti.
		Välkkyy	Välkkyy	Välkkyy	Häiriö, ota yhteys huoltoon

## 6.2. Asennus ATA-sovittimeen

GSM-päätelaite kytkettiin ATA-sovittimeen, jonka portit ovat FXS-portteja, joten GSM-päätelaitteessa käytettiin EXT-porttia. Kun kaapeli oli kytketty, GSM-päätelaite käynnistettiin EXT-tilassa, jolloin LED 2 syttyi päälle. Tämän jälkeen GSM-päätelaitteelle konfiguroitiin SIP-kanava sip.conf-tiedostoon. Asteriskin komentoriviltä tarkistettiin *sip show peers* komennolla, että ATA-sovittimen puhelinportteihin asennetut laitteet kirjautuvat puhepalvelimelle. Esimerkissä 7 on sip.conf-tiedoston konfiguraatiot Nokia 22 PBX GSM päätelaitetta varten.

[304]

*type=friend ; Kanavan tyyppi*

*context=gateway*



Esimerkin 9 konfiguroinneissa on oletettu, että B-tilaajan puhelinnumero on 6-15 numeroa pitkä. Tässä työssä julkisen puhelinverkon suuntanumeroksi valittiin 0-alkuliite. Soittaessa 0-alkuiseen 6-15 numeroa pitkään puhelinnumeroon puhelu ohjataan julkiseen puhelinverkkoon. Tämä onnistuu soittamalla GSM-päätelaitteelle, jonka vastattua puheluun Asterisk lähettää DTFM-äänivalintana A-tilaajan syöttämän puhelinnumeron etu nolaa lukuun ottamatta. Tämän lisäksi valittaessa alanumero 888 saadaan puhekanava auki GSM-päätelaitteen ja A-tilaajan puhelimen välille, jonka jälkeen A-tilaaja voi manuaalisesti syöttää B-tilaajan puhelinnumeron.

GSM-päätelaitteen kanssa tulee ongelmia julkisesta puhelinverkosta sisään tulevien puheluiden osalta, koska sillä ei voida toteuttaa ohivalintaa. GSM-päätelaitteen SIM-kortin puhelinnumeron takana on siis koko puhepalvelimen käyttäjäkanta. GSM-päätelaite ohjaa julkisesta puhelinverkosta vastaanotetut puhelut Asteriskille alanumeroon 200. Numeroanalyysissä (extension.conf) on tämän alanumeron kohdalla esimerkin 10 mukaiset konfiguraatiot.

*[gateway]*

*exten => \_200,1,Answer()*

*exten => \_200,n,Playback(welcome)*

*exten => \_200,n,DISA(no-password,default)*

*exten => \_200,n,Hangup()*

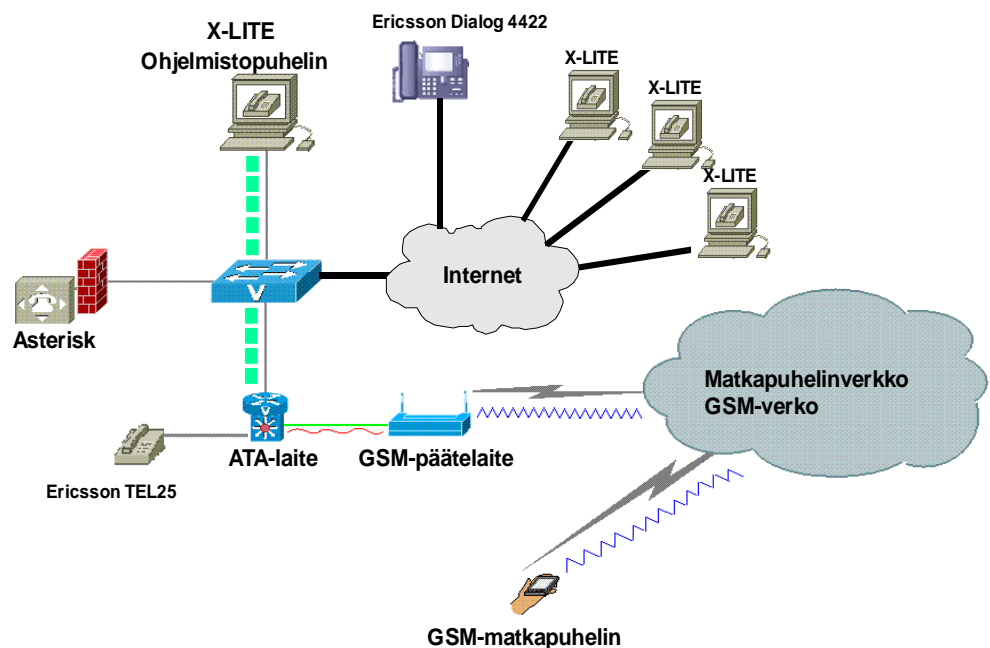
*Esimerkki 10. Asterisk:n saapuvat puhelut.*

Julkisesta puhelinverkosta saapuvat puhelut ohjataan DISA-numeroon, joka on yksi monista puhelinvaihteiden ominaisuuksista. DISA-numeroon soittamalla A-tilaaja kirjautuu puhelinvaihteeseen ja puhelun ollessa käynnissä A-tilaaja toimii DISA-numeron välityksellä puhelinvaihteen alaliittymänä. DISA-numeroon kirjaututtua A-tilaajan tulee antaa alanumero, johon halutaan soittaa ja #-merkillä lopetetaan valinta. Tämän jälkeen Asterisk etsii annetun alanumeron numeroanalyysistään ja yhdistää puhelun. DISA-numeroille voidaan antaa salasana, jotta kuka tahansa ei pääse kirjautumaan puhelinvaihteeseen.

### 6.3. Toiminnan testaus ja analysointi

Tässä työssä toteutetussa VoIP-verkossa julkiseen puhelinverkkoon lähtevät puhelut voidaan valita automaattisesti, jolloin julkisen puhelinnumeron eteen

liitetään julkisen puhelinverkon suuntanumero 0 tai manuaalisesti soittamalla alanumeroon 888, josta syötetään uusi valintaääni, jonka jälkeen voidaan syöttää soitettava julkinen numero. Merkinantona käytetään ohjelmistopuhelimen ja ATA-sovittimen välillä SIP-merkinantoa sekä puhemedia siirretään RTP-virtana. ATA-sovittimen ja GSM-päätelaitteen välillä suoritetaan analoginen merkinanto ja puhekanava avataan ATA-sovittimen ja GSM-päätelaitteen välille, jolloin puhesignaali on analoginen äänisignaali. Lopulta GSM-päätelaite suorittaa merkinantoa matkapuhelinverkkoon. GSM-päätelaitteen reitittäessä puheluita se toimii matkapuhelinverkossa tavallisen puhelimen tavoin (kuva 3).



Kuva 16. Puhelun kulku ohjelmistopuhelimesta matkapuhelimeen.

Käytetyillä konfiguroinneilla puhelut ohjataan ATA-sovittimen toiseen FXS-porttiin, johon on konfiguroitu alanumero 304. ATA-sovitin soittaa GSM-laitteelle, joka vastaa puheluun välittömästi. Näin avataan SIP-istunto Asterisk:n ja ATA-purkin välille, sekä analoginen puhekanava ATA-sovittimen GSM-päätelaite välille, jonka jälkeen A-tilaajalle soitetaan valintaääntä tai Asterisk lähettää soitettavan numeron DTFM-äänivalintana. Numerovalinta perustuu DTFM-tekniikkaan, joten SIP-liittymien tulee käyttää G. 711 alaw tai G. 711 ulaw koodekkia. Muilla koodekeilla annetut äänivalinnat vääristyvät, kun ATA-sovitin muuttaa RTP-paketit analogiseksi signaaliksi.

Puheluiden dataverkossa tapahtuvaa liikennettä tutkittiin syvällisemmin otamalla pakettikaappauksia Wireshark-ohjelmistolla. Näistä kaappauksista pystyttiin kokoamaan miten SIP-merkinanto toimii toteutetussa verkossa.

### *Ohjelmistopuhelimesta soitettu puhelu matkapuhelimeen*

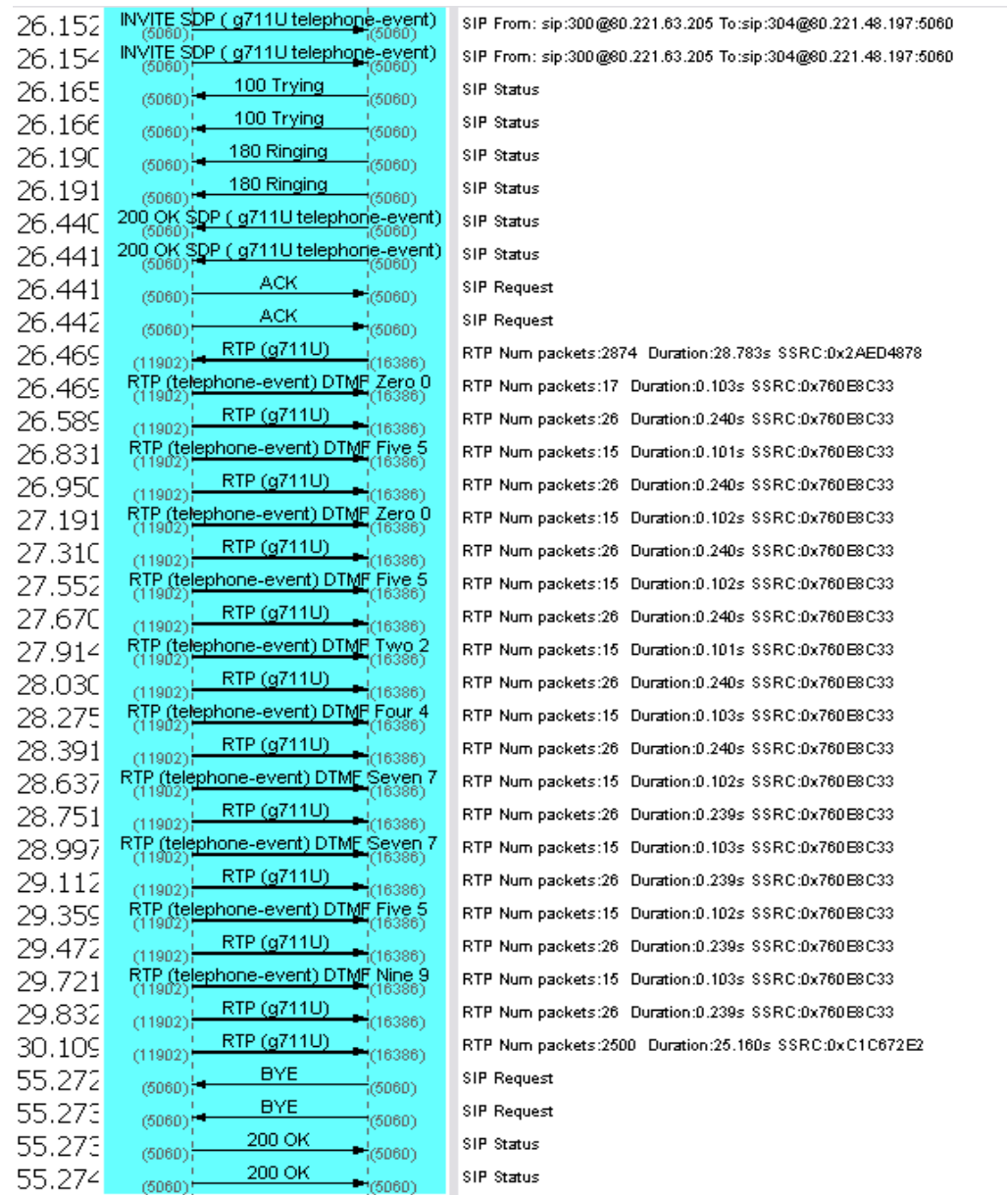
Tässä työssä tehdyissä mittauksissa huomattiin, että ohjelmistopuhelimesta soittaessa matkapuhelimeen merkinanto jakautuu kahteen vaiheeseen. Puhelu soitettiin alanumerosta 300 ja GSM-päätelaite oli sidottu alanumeroon 304. Ensimmäisessä vaiheessa ohjelmistopuhelin ja Asterisk neuvottelevat istunnon tyyppin ja käytettävät puhekoodekit. Tämän jälkeen Asterisk etsii numeroanalyysistä mihin puhelu pitää ohjata ja alkaa hälyttää alanumeroa 304, joka vastaa puheluun ja istunto avataan. Tämä jälkeen siirrytään merkinannon toiseen vaiheeseen. Kuvassa 17 on esitetty merkinannon ensimmäinen vaihe.



*Kuva 17. SIP-merkinannon ensimmäinen vaihe.*

Kuvasta 17 nähdään, että hieman ennen merkinannon ensimmäisen vaiheen päättymistä A-tilaaja kuvaa istunnon alaliittymälle 304. Tämän jälkeen alanumero 304 lähettää vastaukset yritetään, hälytetään ja käytettävä koodi on g.711 ulaw, joihin vastataan hyväksyvästi. Tämän jälkeen istunto

avataan ja B-tilaajan numero lähetetään äänivalintana alanumerolle 304. Tämän jälkeen puhemediaa siirtyy tilaajien välillä, kunnes kummatkin merkinnatvaiheet puretaan alaliittymän 304 toimesta vuoronperään aloittaen toisesta vaiheesta.



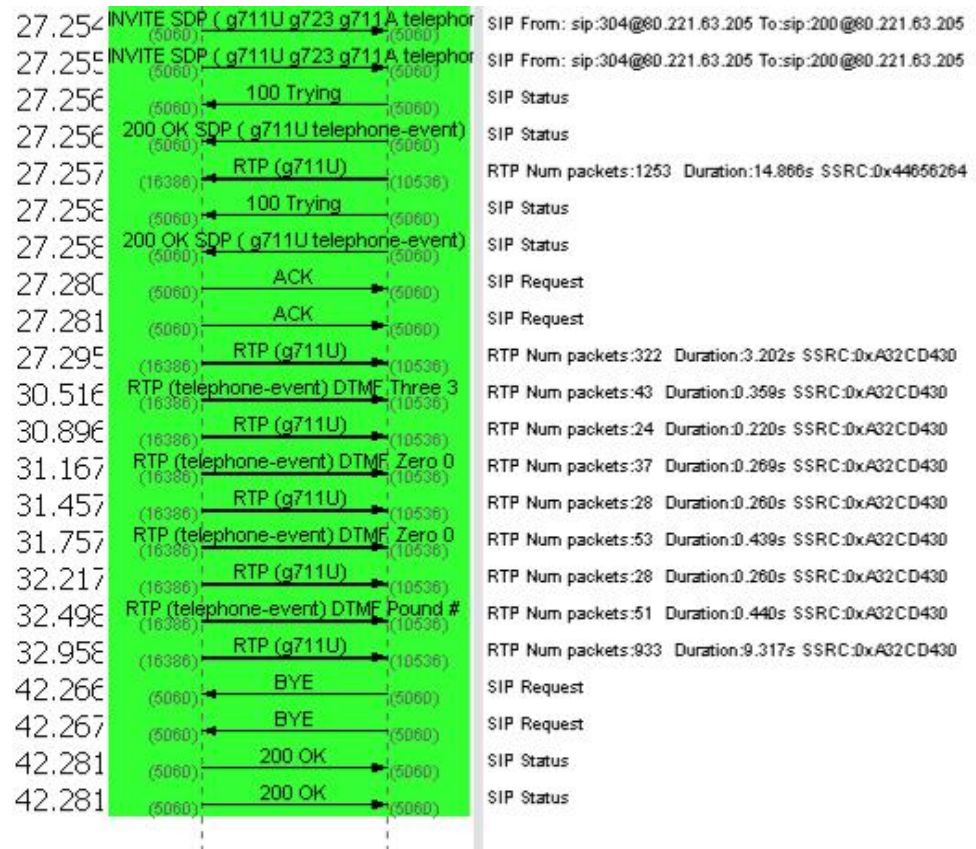
Kuva 18. SIP-merkinannon toinen vaihe.

Kuvasta 18 huomataan, että Wireshark tunnistaa RTP-pakettien sisältämän DTMF-äänivalinnan, joten voimme selvittää mihin numeroon ohjelmistopuhelimesta soitetaan. Liitteessä 4 on puhelussa käytetyt SIP-viestit, jotka koottiin talteen käyttäen Asteriskin komentotulkkaa SIP-vianetsintätilassa. Liitteen 4 viesteistä huomataan mielenkiintoisia seikkoja, kuten miten tarkkaan SIP-viesteissä on määritelty agenttina tai palvelimena toimivan laitteen tiedot.

Cisco Systems ATA-sovitin ja CounterPath X-lite ohjelmistopuhelin tunnisteetaan valmistajan ja version tarkkuudella.

### *Matkapuhelimesta soitettu puhelu ohjelmistopuhelimeen*

Mittauksissa huomattiin, että myös sisään tulevat puhelut jakaantuvat kahteen merkinantovaiheeseen. Ensimmäisessä vaiheessa alanumero 304 hälyttää alanumeroa 200, joka on tarkoitettu sisään tulevia puheluita varten. Merkinannossa yritetään suoraan alanumeroa 200, jonka vastattua avataan puhekanava. Hetken päästä alanumerolle annetaan äänivalinnalla se alanumero, johon A-tilaaja haluaa soittaa. Tämän jälkeen siirrytään merkinannon toiseen vaiheeseen.

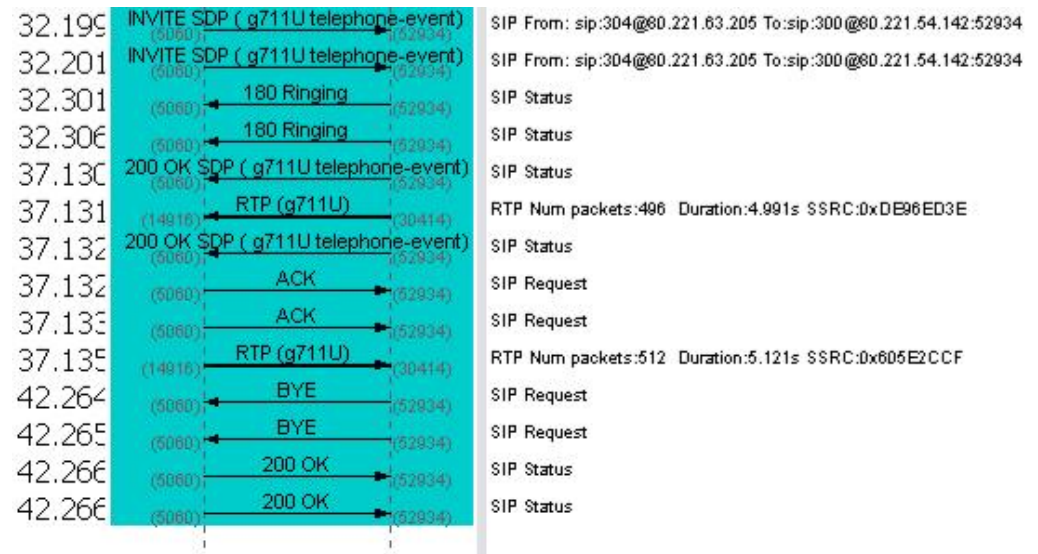


*Kuva 19. SIP-merkinannon ensimmäinen vaihe.*

Kuvasta 19 nähdään, että Wireshark tunnistaa annetun DISA-valinnan eli mihin puhepalvelimen sisäiseen numeroon soitetaan, joka tällä kertaa lähetetään Asterisk-puhepalvelimessa olevalle alanumerolle 200. Merkinannon toisessa vaiheessa istunnon kuvauksen jälkeen alanumero 300 ilmoittaa, että puhelin soi. B-tilaajan vastatessa määrätään käytettävä puhekoodekki ja



aloitetaan median siirto tilaajien välillä. Lopuksi istunto puretaan alanumeron 300 toimesta alkaen toisesta merkinantovaiheesta.



Kuva 20. SIP-merkinannon toinen vaihe.

Verrattaessa kuvia 17 ja 18 sekä kuvia 19 ja 20 huomataan, että vastaanotettavat puhelut aiheuttavat vähemmän merkinantoviestejä verrattuna soitettaviin puheluihin. Tämä on mielenkiintoinen huomio, sillä molemmat puhelut muodostetaan kahdessa merkinantovaiheessa ja niiden muodostus on teknisesti toteutettu samalla tavalla eli lähettämällä B-tilaajan numero äänivalinnalla avattuun puhekanavaan.

#### 6.4. Hätäliikenneohjaukset

Hätäliikenneohjauksilla pidetään huolta, että käyttäjien hätäpuhelut menevät käyttäjän maantieteellisen sijainnin mukaan paikalliseen hätäkeskukseen, jotta hätäkeskus hälyttää pelastushenkilökunnan oikeaan osoitteeseen. Puhelinvaihteeseen ei tarvitse erikseen konfiguroida hätäliikenneohjauksista, mikäli kaikki tilaajat sijaitsevat maantieteellisesti vaihdeliittymän kanssa saman hätäkeskuksen piirissä. Puhelinvaihteverkoissa voi kuitenkin olla maantieteelliseltä sijainniltaan vaihtelevia tilaajia kuten IP-puhelimia tai pienkonttoreita, joiden puhelut ohjataan päävaihteen kautta julkiseen puhelinverkkoon. Esimerkiksi edellä mainituissa tapauksissa hätäliikenne ohjauksien toteuttaminen on puhelinvaihteen eli yritysverkon haltijan vastuulla. [13.]

Viestintäviraston suosituksessa 309/2007 S määritellään suositukset yritysverkon hätäpuheluiden hätäliikenne ohjauksille. Yritysverkoksi lasketaan



suosituksen mukaan kaikki yksityiset puhelinverkot, kuten tässä työssä toteutettu puhepalvelimen käyttäjäkanta. Alla on ote Viestintäviraston suosituksesta 309/2007 S.

Yritysverkon soittajan valitessa 112:n tai 10022:n yritysverkossa muodostettu yleiseen verkkoon lähtevä ohjausnumero on seuraava:

3979 abc 112 (soitto 112:een ja 10022:een)

3979 on Viestintäviraston tähän tarkoitukseen kaikilla telealueilla varaama tilaajanumeroalueen osa

abc = hätäkeskuksen sijaintikunnan kuntanumero

Yritysverkossa muodostettu ohjausnumero muutetaan siinä yleisenpuhelinverkon keskuksessa, johon yritysverkko on liitetty, määräyksen Viestintävirasto 32 J/2007 M yleisen puhelinverkon numeroinnista mukaiseksi hätäliikenteen heksadesimaaliseksi ohjausnumeroksi. [13.]

Tämän työn kannalta ongelmana on se, että yhteys julkiseen puhelinverkkoon on toteutettu GSM-päätelaitteen avulla, jolloin puhelut ohjautuvat GSM-verkkoon. Tämä ansiosta työn hätäliikenne ohjauksien toteuttaminen on ongelmallista. GSM-verkossa käytetään erilaisia ohjausnumeroita kuin kiinteänpuhelinverkon keskuksissa. Viestintäviraston samassa suosituksessa mainitaan matkaviestimistä seuraavaa.

Mikäli yritysverkko on toteutettu matkaviestimillä, suositellaan, että matkaviestinoperaattori ohjaa yritysverkon matkaviestimistä soitetut hätäpuhelut suoraan matkaviestinverkon kautta hätäkeskukseen. Kutsuvana numerona näytetään tässä tapauksessa kyseisen liittymän matkaviestinnumero. [13.]

Tämän työn kannalta tämä ei auta tilannetta, koska toteutetun yritysverkon kaikki hätäpuhelut ohjataan siihen hätäkeskukseen, jonka alueella GSM-päätelaite sijaitsee maantieteellisesti. Työssä toteutettua yksityistä puhelinverkkoa voidaan kuitenkin pitää toissijaisena, koska suurin osa käyttäjistä käyttää ohjelmistopuhelinta käyttäessään tietokonetta.

Käyttäjille ilmoitettiin puhelinjärjestelmän puutteista ja heitä neuvottiin käyttämään henkilökohtaista matkapuhelin hätäpuheluiden soittamiseen. Tulevissa jatkokehitys projekteissa pyritään poistamaan tämä heikkous puhelinjärjestelmästä, joten tätä varten tehtiin alkuvalmisteluita. Seuraavassa vielä yksi lainaus Viestintäviraston suosituksesta 309/2007 S

Viestintävirasto suosittelee, että yritysverkon alaliittymästä voidaan soittaa hätänumeroihin sekä valitsemalla suoraan hätänumero että valitsemalla ensin suunta (keskusjohto) yleiseen puhelinverkkoon ja sen jälkeen hätänumero 112 tai 10022. [13.]

Yllämainittu suositus perustuu siihen, että hätätilanteessa paniikissa oleva käyttäjä ei muista valita julkisen verkon suuntanumeroa 0. Tämä toteutettiin Asterisk:ssa erittelemällä hätänumerot muista alanumeroista ja lisäämällä esimerkin 11 mukaiset rivit extension.conf tiedostoon.

*[hata]*

```
exten => _112,1,Dial(SIP/304/60,rD(${EXTEN})
```

```
exten => _112,n,Hangup()
```

```
exten => _0112,1,Dial(SIP/304/60,rD(${EXTEN:1})
```

```
exten => _0112,n,Hangup()
```

```
exten => _10022,1,Dial(SIP/304/60,rD(${EXTEN})
```

```
exten => _10022,n,Hangup()
```

```
exten => _010022,1,Dial(SIP/304/60,rD(${EXTEN:1})
```

```
exten => _010022,n,Hangup()
```

*Esimerkki 11. Hätäpuhelut ilman julkisen puhelinverkon suuntanumeroa.*

Esimerkissä 11 mainituilla konfiguroinneilla pidetään huolta, että hätäpuhelut lähtevät julkiseen puhelinverkkoon, vaikka käyttäjä ei valitse julkisen verkon suuntanumeroa 0. Numeroalue 1xx varattiin aikaisemmin järjestelmän omia ohjauksia varten, jotta käyttäjät eivät vahingossa soita hätänumeroon.

Keskusjohdoilla julkiseen puhelinverkkoon yhdistetyt puhelinvaihteet konfiguroidaan lisäämään Viestintäviraston suosituksen mukainen etuliite lähetettävän numeron eteen, jotta puhelu ohjautuu oikeaan hätäkeskukseen. Tilaaajat tunnistetaan toisistaan tilaajaluokkien avulla, jolloin jokaisella tilaajaluokalla on oma hätäliikenneohjauksen etuliite. Yritys käytössä olevasta puhelinvaihteverkoissa IP-puhelimet saavat hätäliikenne ohjaukset konfiguraatio-tiedostosta, jonka ne hakevat tiedostopalvelimelta, IP-puhelimien IP-osoitteet on usein jaettu toimipisteen perusteella eri aliverkkoihin tai toimipiste kohtaisiin verkkotunnuksiin. Tämän ansiosta tiedostopalvelimen konfiguraatitiedostot voidaan jakaa toimipistekohtaisiin kansioihin IP-osoitteen tai DNS-nimen mukaan, jolloin jokaiselle toimipisteelle saadaan oikeat hätäliikenneohjaukset. Konfiguraatitiedostojen sisältö ja niiden jakamiseen käytetty protokolla vaihtelee riippuen laitevalmistajasta.

## 7. PALVELIMEN VERRKOPALVELUT

Asterisk puhepalvelimelle asennettiin IP-pohjaisen dataverkon verkkopalveluita, jotta VoIP-verkosta saataisiin erilaisiin tilanteisiin skaalautuvampi. Osa verkkopalveluista on välttämättömiä isoissa VoIP-verkoissa ja osa parantaa verkon toimintaa. Tässä osiossa esitellään muutamia verkkopalveluita, joista on hyötyä VoIP-verkoissa.

### 7.1. HTTP

HTTP on verkkosivujen datan siirtoon käytettävä protokolla, jolla voidaan siirtää ASCII tai binaaria dataa. HTTP standardoitiin alkuaan RFC 1945 , mutta nykyään käytetään uudempaa HTTP1.1 versiota protokollasta, joka esiteltiin RFC 2616:ssä. Salattua liikennettä varten kehitettiin HTTPS-protokolla, joka toimii SSL:n päällä ja on standardoitu RFC 2660. Virallisesti HTTP käyttää TCP/UDP porttia 80 ja HTTPS TCP/UDP porttia 443. [7, s. 216 – 219.]

AsteriskNOW-paketissa on Apache-palvelin deemoni valmiiksi asennettuna ja sillä on tiedostoja varten käytössä kansio ' /var/www/html '. Työssä asennettua IP-puhelinta varten kansioon /var/www/html luotiin oikean tyyppinen alihakemistopuu, josta IP-puhelin osaa hakea verkko-osoitteen ja puhelinmallin perusteella oikeat tiedostot.

### 7.2. DHCP

DHCP on IETF:n RFC 1531:ssä standardoitu protokolla, jonka avulla IP-osoitteita voidaan jakaa automaattisesti palvelimelta asiakaskoneen pyynnöstä. Asiakaskone lähettää DHCP etsintäviestejä yleislähetystenä käyttäen UDP porttia 68, joihin DHCP-palvelin vastaa tarjousviestillä. Tarjousviesti sisältää sopivan asiakaskoneen IP-osoitteen, DHCP-palvelimen IP-osoitteen ja asiakaskoneen MAC-osoitteen. Tarjousviestit lähetetään yleislähetystenä porttiin 67. Asiakaslaite voi saada useita tarjousviestejä, joista se valitsee ensimmäisen ja lähettää DHCP-pyyynnön yleislähetystenä, josta DHCP-palvelimet pystyvät selvittämään mikä tarjous otettiin vastaan. Tämä kertoo hyväksytyyn tarjoukseen lähettäneelle DHCP-palvelimelle, että IP-osoite tulee lukita ja muille DHCP-palvelimille, että heidän tarjoukset hylättiin ja tarjottu IP-osoite on edelleen vapaa. Tämän jälkeen hyväksytyyn tarjoukseen lähetetään DHCP-vahvistusviesti, jossa määritellään asiakaskoneen IP-osoite,

aliverkon peite, kuinka kauan kyseinen IP-osoite on voimassa ja muuta asiakaslaitteelle olennaisia tietoja, kuten oletusreitittimen IP-osoite, DNS-palvelimen osoite ja muita konfigurointeja. DHCP kehitettiin korvaamaan vanhempi Bootstrap Protocol, jota aikaisemmin käytettiin jakamaan IP-osoitteita dynaamisesti. Nykyään IP-verkoissa on satoja asiakaskoneita, joten DHCP on käytössä lähes jokaisessa verkossa. [14, s. 280 – 283.]

IP-puhelimet voivat saavat DHCP-palvelimelta IP-osoitteen lisäksi tiedon mistä IP-osoitteesta käynnistystiedostot sisältävä tiedostopalvelin löytyy. Tiedostopalvelimen protokolla riippuu laitevalmistajasta, mutta tässä voidaan käyttää esimerkiksi TFTP- tai HTTP-palvelinta. Tässä työssä asennettiin puhelipalvelimelle DHCP-taustaprosessi tulevia projekteja varten, mutta sitä ei vielä otettu käyttöön.

### 7.3. NTP

NTP on IP-pohjaisessa dataverkossa aikatiedon synkronointiin käytetty protokolla. NTP on vanhimpia protokollia, josta uusin versio on 4. NTP on standardoitu RFC 778, RFC 891, RFC 956 ja RFC 1305 sekä sillä on virallisesti käytössä UDP portti 123. NTP:n avulla verkon laitteilla on keskenään sama kellonaika, jota käytetään tietoturva toiminnoissa ja verkonhallinnassa. Mikäli verkon laitteiden kellonajat vaihtelevat suuresti verkonhallinta on hyvin hankalaa, koska lokitiedostoiden sisältöön ei voida luottaa, sillä niissä näkyvät aikaleimat eivät täsmää. Lisäksi useat protokollat merkkäavat paketteihin aikaleiman lähetysajan perusteella, joiden avulla vastaanottava laite voi päätellä, onko paketti oikea, käytettävissä vai väärennetty. [7, s. 292.]

Tässä työssä otettiin NTP-palvelin käyttöön käytännöllisemmistä syistä, sillä asennettuun Ericsson Dialog 4422 IP-puhelin haluttiin saada pysymään oikeassa ajassa. Puhelimien kellonajat ovat tärkeitä VoIP-verkossa, koska yritysten puhelinpalvelut ovat ajastettu sulkeutumaan tiettyyn kellon aikaan ja työntekijät usein katsovat puhelimen kellosta, milloin pitää lähteä töistä kotiin. Mikäli puhepalvelimen kello on 15 minuuttia edellä ja asiakas soittaa kello 16.50 palveluun, ei hänen puhelu yhdisty enää asiakaspalvelijalle, vaan asiakkaalle soitetaan automaattinen viesti, jossa neuvotaan soittamaan uudestaan palveluaikana.

## 7.4. TFTP

TFTP on UDP:n päällä toimiva tiedonsiirtoprotokolla, joka kopioi tiedostoja palvelimelta asiakasohjelmalle. TFTP on FTP-protokollasta kevyempi versio, jolla on hyvin rajatut ominaisuudet tiedonsiirron kannalta, mutta TFTP vie vähän resursseja, joten sitä voidaan käyttää hyvin pienissä laitteissa. TFTP:tä pidetään myös tietoturvariskinä, koska se ei sisällä kirjautumistointoja. TFTP käyttää UDP-porttia 69. TFTP kuvataan IETF:n standardissa RFC 1350. [14, s. 176] TFTP:tä käytetään IP-puheluiden käynnistystiedostojen jakamiseksi palvelimelta puhelimille ja puhelinkohtaisten puhelinluetteloiden tallentamiseen palvelimelle. Käynnistystiedostoja ovat puhelimen konfiguraatitiedostot, kielitiedostot ja firmware-tiedostot.

Tässä työssä otettiin TFTP-palvelu käyttöön, koska ATA-sovitinta on helppompaa hallita, konfiguroida ja päivittää TFTP-palvelimelta. Työssä käytetty vsftpd-tasutaprosessi sisältyi AsteriskNOW-pakettiin, joten se oli asennuksen jälkeen oletusasetuksilla toiminnassa.

## 8. TIETOTURVA

Tässä osiossa tutkitaan Asterisk-puhepalvelimen tietoturvaa ja mitä toimenpiteitä tulisi tehdä, jotta tietoturvaa saataisiin parannettua. Kotikäytössä olevalle puhepalvelimelle tietoturva ei ole yhtä kriittistä kuin yrityksen tai muun organisaation käytössä olevan puhepalvelimen. Käyttäjien puhelut halutaan turvata, joten tässä työssä muutamia tietoturvaa parantavia parannuksia palvelimeen.

### 8.1. Mahdolliset uhat

VoIP-verkkoa voidaan pitää hyökkäysalttiina alueena, koska siellä esiintyy dataverkon ja puheverkon uhkia. Puheluita voidaan salakuunnella, puhelin tai koko puhepalvelin voidaan kaapata, verkkoa voidaan kuormittaa ja verkko voi tulla palvelunesto hyökkäyksten kohteeksi.

Palvelunestohyökkäyksillä pyritään estämään verkon käyttäjiä käyttämästä verkon tarjoamia palveluita. Palvelunestohyökkäyksistä voi kärsiä kaikki IP-pohjaiset verkkopalvelut. Palvelunestohyökkäykset vaihtelevat riippuen siitä mikä palvelu on hyökkäyksen kohteena, mutta perusidea on aina sama. Hyökkääjät tulivat hyökättävään verkkoon paketteja yhdestä tai useammasta

ta lähteestä. Hyökkävä verkko joutuu prosessoimaan paketit ja tämä kuormittaa verkkoa. IP-puhelimien ohjelmistot eivät aina ole laadukkaita. Esimerkiksi IP-puhelimen saadessa suuri määrä RTP-paketteja se saattaa jumittua. Jotkut IP-puhelimet myös lakkaavat toimimasta, kun ne ottavat vastaan yli 65534 tavun kokoisen UDP-paketin portista 5060. VoIP-verkkoon kohdistuvat hyökkäykset voivat olla RTP-pakettien tulvimista, huuhaa pakettien tulvimista, merkinannon häiritsemistä vääristetyillä merkinantoprotokollapaketeilla, QoS-määritysten vääristämistä ja prosessointitehoa vaativien pakettien lähettämistä. Palvelunestohyökkäyksiltä on vaikea puolustautua, mutta verkon jakaminen loogisiin osiin VLAN:n avulla, QoS-määritykset ja hyvin konfiguroidut palomuurit auttavat verkkoa suojautumaan hyökkäyksiltä. [7, s. 240 – 248]

Toinen tietoturvariski on verkossa olevien laitteiden tai liikenteen kaappaus. Kaapattavat laitteet voivat olla puhelimia tai kokonaisia palvelimia, joita kaappaaja käyttää hyväksi omiin tarkoituksiinsa. Kaapatuilla laitteilla voidaan soittaa ulkomaille tai palvelunumeroihin, jotta puhelimen omistajalle saataisiin kerättyä mahdollisimman suuri puhelinlasku. Palvelunumerot voivat olla kaappaajan omistamia, joista hän pyrkii hankkimaan lisätuloja. Palvelimien kaappauksen estämiseksi voidaan palvelimen tietoturvaa parantaa ja etähallintaa tulee rajata. Puhelimien tietoturva usein vaihtelee laitevalmistajakohdaisesti, mutta numeron sitominen IP-osoitteeseen tai MAC-osoitteeseen estää kaappaajia käyttämästä omaa puhelinta hyökkävässä verkossa. Mikäli numeroa ei sidota mihinkään, tulee puhelimen kirjautumiseen käytettävä salasana ja tunnus olla tarpeeksi vahva. Kaikki mahdollinen puhelimesta lähtevä liikenne tulee myös salata.

Välitävetohyökkäykset ovat kaappaukseen perustuva tietoturvahyökkäyksiä, joissa ulkopuolinen henkilö pyrkii kaappaamaan liikennettä, josta hänelle on jollain tavalla hyötyä. Käytännössä tämä usein on liikenteen salakuuntelua. Tämä tietoturva riski on alkuaan puhelinverkoista ja välitävetohyökkäyksiä joskus kutsutaan epärehelliseksi välittäjäksi. VoIP:n osalta välitävetohyökkäykset ovat puheluiden salakuuntelua. Puheluita voidaan myös haluta nauhoittaa, mikäli yritys tarjoaa puhelinneuvontaa esimerkiksi lakiasioista tai perinnönjakoon liittyen. VoIP-liikenteen kaappaamiseen ja kaapattujen pakettien analysointiin löytyy useita ohjelmia, mutta suurin ongelma hyökkäjälle on, miten päästä kaappaamaan liikennettä näitä ohjelmia käyttäen.

Kaappaaja voi väärentää tietokoneensa MAC-osoitteen ja myrkyttää verkon käyttäjien verkkokorttien ARP-taulukot, jolloin MAC-tason kytkimet lähettävät muualle tarkoitettua liikennettä kaappaajalle. Lisäksi hyökkääjä voi asentaa verkkoon oman puhepalvelimen ja pakottaa puhelimia kirjautumaan sinne, jotta hän voisi ohjata kirjautuneiden puhelimien puhelut kulkemaan hyökkääjän palvelimen kautta oikealle palvelimelle. Hyökkääjä voi myös varastaa numeron tai väärentää numeron soittajan identiteetti kentän, jonka avulla hyökkääjä tekeytyy tietyksi henkilöksi. Välistävetohyökkäyksiltä voidaan välttyä hyvällä median ja merkinannon salaamisella sekä sitomalla puhelimet kirjautumaan vain tietylle palvelimelle ja lisäämällä palvelimelle kriteereitä kirjautuvien puhelimien osalta. [7, s. 248 – 256.]

## 8.2. Palomuri

Palomuri on dataverkon tietoturvakoelementti, jonka tehtävänä on estää ei-luotettua liikennettä pääsemästä palomuurin takana olevaan verkkoon. Palomureja on erityyppisiä riippuen, siitä miten syvällisesti pakettiliikennettä voidaan rajata. Palomuurit pystyvät rajaamaan liikennettä lähettäjän ja kohteen IP-osoitteen perusteella, IP-pakettien käyttämän TCP- tai UDP-portin perusteella tai sovellusten istunnon muodostumiseen käytettävien viestien sisällön perusteella. Liikenteen rajaamisen lisäksi palomuurit hoitavat usein tarvittavat NAT-muunnokset ja toimivat VPN-tunneleiden päätepisteenä. [7, s. 392 – 395.]

VoIP-liikenteen ohjaamista palomuurin läpi tulee välttää aina kun mahdollista, koska VoIP-liikenne vaatii useiden porttien avaamista palomuurista RTP-virtaa varten, kuten taulukosta 8 nähdään. SIP- ja H.323-merkantoprotokollat sekä median siirto käyttävät eri portteja ja ottavat dynaamisesti käyttöön uusia portteja tarpeen mukaan, joten palomuurin konfigurointi tukemaan VoIP-liikennettä on usein hyvin hankalaa. Taulukkoon 8 on suuntaa-antavasti kerätty VoIP-liikenteen käyttämiä UDP/TCP-portteja, joista tuleva liikenne tulee päästää läpi palomuurista. [7, s. 396 – 398.]

Taulukko 8. VoIP-liikenteen käyttämät TCP/UDP-portit.

Merkinanto	Toiminto	Portti	Protokolla
SIP/H.323	RTP	5004	UDP
SIP/H.323	RTCP	5005	UDP
SIP/H.323	RTP/RTCP-virta (voidaan rajata)	1024-65535	UDP
H.323	H.245 merkinanto (voidaan rajata)	1024-65535	TCP
H.323	Portinvartijan löydettävyys	1718	UDP
H.323	Portinvartijan RAS	1719	UDP
H.323	Q.931 merkinanto	1720	TCP
H.323	H.235 turvallisuus merkinanto	1300	TCP
SIP	SIP-merkinanto	5060	TCP
SIP	SIP-merkinanto	5060	UDP
SIP	TLS kryptattu SIP-merkinanto	5061	TCP
IAX2	Merkinanto ja median siirto	4569	UDP
IAX1	Epävirallinen ja vanhentunut IAX	5036	UDP
Kaikki	STUN tekemä NAT-muunnos	3478	UDP
Kaikki	STUN tekemä NAT-muunnos	3478	TCP
Kaikki	TLS-kryptattu STUN	5349	TCP
Kaikki	TLS-kryptattu STUN	5349	UDP

Taulukossa 8 on otettu huomioon SIP-, H323- ja IAX-merkinantoprotokollien käyttämät portit. Riippuen käytettävästä merkinannosta, NAT-muunnoksesta ja salauksesta muut portit voidaan sulkea. STUN-protokollan käyttämät portit vaihtelevat laitevalmistajakohtaisesti ja ne tulee avata, kun liikenne kulkee NAT-muunnoksen läpi, mutta IAX-protokollan osalta tämä vaihtelee tilannekohtaisesti. RTP-virtaa varten avattavien porttien määrä vaihtelee riippuen puhepalvelimen ja IP-puhelimien laitevalmistajasta.

Asteriskille voidaan määritellä RTP-virtaa varten käytössä olevat portit konfiguraatitiedostossa rtp.conf. Esimerkissä 12 näytetään, miten portit rajataan rtp.conf-tiedostossa.

*[general]*

*rtpstart=10000 ;Ensimmäinen käytössä oleva portti*

*rtpend=20000 ;Viimeinen käytössä oleva portti*

*Esimerkki 12. RTP-protokollan käyttämien porttien rajaus.*



Mikäli osa käytössä olevista porteista on suljettuna ja RTP voi dynaamisesti ottaa käyttöön suljettuja portteja. Tällöin media ei kulje päätepisteiden välillä niiden pakettien osalta, jotka käyttävät suljettuja portteja. Taulukon 8 porttien lisäksi laitevalmistajasta ja VoIP-verkon palveluista riippuen voidaan joutua avaamaan muitakin portteja.

Palomuurin kiertämiseen on kehitetty useita temppuja, mutta ehkä yleisin tapa on vuokrata teleoperaattorilta tietoturallinen WAN-verkko, jota käytetään toimipisteiden väliseen dataliikenteeseen. Nämä WAN-verkot käyttävät usein MPLS-tekniikkaa, jonka avulla yritysten toimipisteet voidaan yhdistettään toisiinsa MPLS VPN-tunneleiden avulla, vaikka samaa MPLS-verkkoa käyttäisi monta eri yritystä.

VoIP-puheluiden kannalta tilallinen palomuuuri toimii paremmin, jolloin palomuuuri pitää kirjaa muodostetuista TCP- ja UDP-yhteyksistä ja sallii näihin yhteyksiin kuuluvat paketit. Tämän ansiosta esimerkiksi VoIP-puhelun merkinannon perusteella tilallinen palomuuuri voi päätellä päästettäväksi saapuva liikenne palomuurista läpi. Tilalliset palomuurit tukevat usein ainakin SIP- ja H.323-merkinantoprotokollia. Tilattomat palomuurit toimivat vain suodattimina, joille määritellään mistä porteista tuleva liikenne sallitaan läpi, joten tilallisia palomuuureja voidaan pitää parempana ratkaisuna VoIP-verkoissa.

### 8.3. Puhepalvelimeen tietoturva

Puhepalvelimen tietoturvan parantaminen kannattaa aloittaa käyttöjärjestelmän tietoturvan parantamisesta. Työssä käytetty AsteriskNOW-asennuspaketti sisälsi räätälöidyn version CentOS-käyttöjärjestelmästä, josta oli jo valmiiksi poistettu turhia ominaisuuksia. Työssä esitellään muutama toimenpide, joilla Linux-palvelimen tietoturvaa voidaan parantaa.

Puhepalvelimelta kannattaa ottaa pois käytöstä kaikki verkkopalvelut, jotka eivät ole käytössä. *Service --status-all ja ps aux* komennoilla voi selvittää, mitkä palvelut ovat käytössä. Näiden verkkopalveluiden ominaisuuksia ja käynnistymisiä pystyy muuttamaan *inet-* ja *xinet-*palveluiden konfiguraatio-tiedostoja kuten */etc/xinetd.conf*. Lisäksi *chkconfig* komennolla voi poistaa palvelimen käynnistyessä käynnistettäviä palveluita. Se, mitä palveluita kannattaa ottaa pois ja miten ne otetaan pois käytöstä, vaihtelee puhepalvelin-kohtaisesti, mutta esimerkiksi sähköpostipalvelut kuten *popd* ja *imafd* voidaan usein ottaa huoletta pois käytöstä. [7, s.281 – 283.]

Palveluiden poiston jälkeen kannattaa tarkistaa, että järjestelmälokit ovat kunnossa. Linux-käyttöjärjestelmän järjestelmäloki taustaprosessin konfigurointitiedosto on `/etc/syslog.conf` ja järjestelmälokit tulevat kansioon `/var/log`. Lokitiedot ovat äärimäisen tärkeitä vian korjauksessa tai palvelimen häiriöiden paikannuksessa, joten järjestelmälokien tietoja voidaan tarkentaa tarpeen mukaan. Käyttäjien oikeuksia kannattaa rajoittaa järjestelmään sopivaksi, erityisesti vain pääkäyttäjän käytössä olevien komentojen kohdalta. Tämä onnistuu esimerkiksi luomalla järjestelmään uusi käyttäjäryhmän, jonka jäsenillä on oikeus siirtyä pääkäyttäjäksi komennolla `/bin/su`. Kaikilta muilta käyttäjiltä ja käyttäjäryhmiltä tämän komennon suorittaminen estetään. Tämän jälkeen joidenkin komentojen suoritusoikeuksia on hyvä alentaa, koska niitä käyttäjät tarvitsevat niitä usein, eikä tarvitse turhaan siirtyä pääkäyttäjäksi. Esimerkiksi seuraavien komentojen suoritusoikeuksia kannattaa alentaa kaikille järjestelmää hallitseville käyttäjille `ping`, `ping6`, `mount`, `umount`, `traceroute` ja `traceroute6`. [7, s. 283 – 288.]

Näiden toimenpiteiden lisäksi palvelimesta kannattaa poistaa oletuksena asennettavia, mutta turhia tiedostoja ja ohjelmia. Palvelunestohyökkäyksiä varalta kannattaa rajata järjestelmän prosessien resursseja ja poistaa käytöstä käyttämättömiä toimintoja kuten tulostaminen. Näiden lisäksi käyttöjärjestelmäkohtaisia virityksiä löytyy paljon. [7, s. 288 – 289.] Palvelimelle voidaan myös asentaa palomuri tai muita verkkoliikennettä rajaavia ohjelmia, mutta nämä usein kannattaa asentaa erilliseen laitteeseen, koska palvelimet sijaitsevat usein tähän tarkoitukseen sopimattomassa osassa verkkoa. Kotikäytössä voidaan ottaa käyttöön Linux-käyttöjärjestelmän iptables-palomuri, josta löytyy lisätietoa esimerkiksi iptables manuaalisivuilta.

Asterisk ohjelmaa usein ajetaan pääkäyttäjänä, vaikka tätä ei suositella, koska se on tietoturvariski. Myös AsteriskNOW-asennuspaketti asentaa Asteriskin ajettavaksi pääkäyttäjänä. Käyttäjän muutokseen tarvittavat toimenpiteet vaihtelevat käyttöjärjestelmäkohtaisesti. Käytännössä tämä kuitenkin voidaan toteuttaa lisäämällä järjestelmään asterisk-käyttäjä, joka asentaa itselleen Asteriskin. Tämän jälkeen käyttöjärjestelmän käynnistyskomentosarjoihin muutetaan Asterisk-prosessi käynnistettäväksi asterisk-käyttäjänä pääkäyttäjän sijaan. [10, s. 295 – 298.]

#### 8.4. Puheluiden salaus ja verkkoelementtien tietoturva

VoIP-puheluiden salaaminen voidaan jakaa kahteen osaan merkinannon salaamiseen ja median siirron salaamiseen. Salaamisella tarkoitetaan lähetettävien pakettien kryptaamista ymmärtämättömäksi. SIP-pakettien sisältö voidaan salata käyttäen TLS-protokollaa. TLS on SSLv3-protokollaan perustuva IETF:n RFC2246:ssä standardoima tekniikka, jolla voidaan luoda tietoturvallinen läpinäkyvä kanavan kahden päätepisteen välille. Läpinäkyvyydellä tarkoitetaan sitä, että kanavassa kulkevaa dataa ei muokata mitenkään. Tämän ansiosta TLS soveltuu hyvin TCP-sovelluksiin ja sitä voidaan käyttää lähes kaikkien TCP-sovellusten kanssa. TLS perustuu sertifikaattivaihto tekniikkaan. [7, s. 417 – 420.]

Puhemedia voidaan salata esimerkiksi SRTP:n avulla, joka on määritelty RFC 3711:ssä. SRTP toimii RTP-mediaa lähettävän sovelluksen ja RTP-pakettien siirron välissä. Sovellukselta tulevat paketit kryptataan salatuksi käytetään AES-algoritmia symmetristen avainten avulla. Kryptatusta medias- ta luodaan RTP-paketti, joka lähetetään verkon yli vastaanottavalle laitteelle. Vastaanottava laite käyttää omaa symmetristä avaintaan kryptauksen purkamiseen ennen median lähettämistä omalle RTP-sovellukselleen. SRTP-protokollan ongelmana on symmetristen avainten hallinta ja välittäminen laitteiden välillä vaihtelee VoIP-verkon laitteiden ja sovellusten valmistajasta. [7, s. 420 – 422.]

Tässä työssä käytössä olevat verkkolaitteet olivat ATA-sovitin, kytkin ja loppukäyttäjien puhelimet. Käytössä oleva kytkin ei ole hallittava, joten sen osalta ei toimenpiteitä suoritettu. Loppukäyttäjien puhelimet koostuivat pääasiassa ilmaisista ohjelmistopuhelimista, joiden omaisuudet olivat hyvin rajattuja tai niissä oli valmistajakohtaisia toimintoja. Asterisk ei virallisesti tue SIP-merkinannon ja RTP-mediaan salausta, mutta ne voidaan ottaa käyttöön kolmannen osapuolen sovellusten avulla. Puhelimiin rajoitusten ansiosta puhemediaan ja merkinannon salaus ei tämän hetken valinnoilla onnistu. ATA-sovittimelle kuitenkin piti tehdä useita toimenpiteitä, koska oletusasetuksilla sen tietoturva on hälyttävän olematon.

ATA-sovittimen WWW-konfigurointi ei oletusasetuksilla vaadi kirjautumista, joten ATA-sovittimen asetusten muuttaminen vaatii vain IP-osoitteen selvittämisen. Tästä syystä ATA-sovittimeen asetettiin alkuvaiheessa salasana, mutta työn päätteeksi WWW-selaimella konfigurointi otettiin pois käytöstä ja

jatkossa konfigurointiin käytetään TFTP-palvelimelta haettavaa konfiguraatiotiedostoa. ATA-sovitin ei tue mitään merkinannon tai mediansiirron salaus tekniikkaa, joten itse puheluita ei voida salata.

## 9. YHTEENVETO JA TULEVAT PROJEKTIT

Tässä työssä huomattiin, että Asterisk-puhepalvelimeen saadaan viritettyä lähes kaikki puhelinvaihteen ominaisuudet. Kotikäytössä Asterisk-palvelimella pystyy oikein toteutettuna säästämään suuren ihmisryhmän puhelinlaskuja, koska ryhmän sisäiset puhelut ovat ilmaisia. Luonnollisesti mitä enemmän käyttäjiä järjestelmällä on ja mitä aktiivisemmin järjestelmää käytetään, sitä enemmän on mahdollista säästää. Asterisk soveltuu hyvin kotikäyttöön ja vaikka Asteriskin tietoturvaominaisuudet todettiin heikoksi, sitä voidaan käyttää Pk-yrityksien puhelinratkaisuna. Työn tekijän oppiman mukaan GPL-lisenssin alla julkaistua versiota Asteriskista ei kuitenkaan voi suositella suurten tai keskisuurten yritysten käyttöön. Lisäksi Asterisk on virittelijälle tai harrastajalle ihanteellinen järjestelmä, mutta huoltohenkilökunnalle sen hallinta voi tulla ongelmalliseksi, sillä huoltohenkilöt eivät välttämättä ymmärrä toistensa tekemiä muutoksia järjestelmään. Omien viritysten lisääminen suurempaan järjestelmää tulisikin estää ja huoltohenkilöiden kanssa tulisi sopia yhteinen ajatusmalli, jolla konfigurointi toteutetaan.

Asennuksen jälkeen palvelin toimii odotusten mukaisesti ja sen jatkokehitystä varten on jo tiedossa useita eri projekteja. Tarkoituksena on kehittää palvelinta monipuolisempi multimedialjärjestelmä sekä asentaa siihen pikaviestintä ja IP-TV-sovelluksia. Asterisk ei tällä hetkellä tue videokonferenssia, mutta mikäli se lisätään järjestelmään tulevaisuudessa ohjelmistopäivityksissä, voidaan myös se ottaa käyttöön asennettuun järjestelmään.

Palvelin sai tällä hetkellä DHCP:ltä IP-osoitteensa, mutta tarkoituksena on hankkia palvelimelle domain-nimi, jotta IP-osoitteen vaihtuminen ei aiheuttaisi uudelleen konfigurointeja. Tätä ei kuitenkaan vielä toteuteta, koska palvelimen fyysinen sijainti ja Internet-liittymän tarjoava teleoperaattori tulevat muuttumaan lähitulevaisuudessa.

Työn toteuttamisessa tähdättiin minimoimaan kustannukset, joita tuli vain testipuheluiden soittamisesta. Tietyillä investoinneilla puhelinjärjestelmän saisi toimimaan paremmin. Työssä käytetty GSM-päätelaite on vanha ja se

tarjoaa vain yhden aikavälin julkiseen puhelinverkkoon, joka riittää vielä tällä hetkellä. Käytössä olevan GSM-päätelaitteen tilalle voitaisiin hankkia kehittyneempi IP-verkkoon asennettava GSM-päätelaite, minkä hinnat ovat 200-400 euron luokkaa.

GSM-päätelaitteella on mahdollista lähettää SMS-viestejä, jonka toteuttaminen nykyisellä laitteistolla on mahdollista. Tähän vaaditaan kuitenkin sopiva välisovellus, joka osaa komentaa GSM-päätelaitetta tietyillä AT-komennoilla, kun GSM-päätelaite toimii modeemina. Tämän tyyppistä sovellusta ei luultavasti löydä mistään, joten se pitää ohjelmoida itse. Yksi tulevaisuuden projekteista onkin saada GSM-päätelaite lähettämään SMS-viesteillä kutsuja ennalta sovittuun puhelinkonferenssiin. Työn tietoturva osiossa huomattiin, että puheluiden salaaminen ei tällä hetkellä onnistu. Tästä syystä ensimmäinen jatkokehitysprojekti on eri ohjelmistopuhelinten tutkiminen ja testaaminen, jotta käyttäjien puhelut saataisiin turvattu.

Puhepalvelimen käyttö on odotettua vilkkaampaa, joten luultavasti palvelimesta on hieman hyötyä myös sen käyttäjille. Kokonaisuutena tämän työn toteuttaminen oli hyödyllinen erityisesti työn toteuttajalle, koska työtä tehdessä oppi paljon uutta aihealueisiin liittyen. Asterisk-palvelimen virittely todettiin opettavaiseksi ja se jäi myös työn toteuttajalle harrastukseksi. Toivottavasti työstä on myös hyötyä sen lukijoille.

## VIITELUETTELO

- [1] Anttalainen, Tarmo, *Introduction to Telecommunications Network Engineering*, Norwood, MA 02062: ARTECH HOUSE, INC., 2003.
- [2] Halsall, Fred, *Multimedia communications – Applications, Networks, Protocols and Standards*, Harlow: Addison-Wesley, 2001.
- [3] Freeman, Roger L., *Telecommunication system engineering*. Fourth edition. New Jersey: A John Wiley & sons Inc., 2004.
- [4] Davidson, Jonathan – Peters, James – Bhatia, Manoj – Kalidindi, Satish – Mukherjee, Sudipto, *Voice over IP Fundamentals*. Second edition. Indianapolis: Cisco Press, 2007.
- [5] Granlund, Kaj, *Langaton tiedonsiirto*, Porvoo: Docendo, 2001.
- [6] Granlund, Kaj, *Tietoliikenne*, Porvoo: Docendo, 2003.
- [7] Porter, Thomas, ym., *Practical VoIP Security*, Rockland: Syngress Publishing, Inc., 2006.
- [8] Finneran, Michael F., *Voice Over WLANs – The Complete Guide*, Oxford: Newnes, 2008.
- [9] Internet Engineering Task Force, RFC 4594 Diffserv [verkkodokumentti, viitattu 4.1.2010]. Saatavissa: <http://tools.ietf.org/html/rfc4594>.
- [10] Meggelen, Jim Van – Madsen, Leif – Smith, Jared, *Asterisk™: The Future of Telephony*. Second edition. Sebastopol: O'Reilly Media, Inc, 2007 (2005).
- [11] Jackson, Benjamin – Clark III, Champ – Chaffin, Larry – Long, Johnny, *Asterisk Hacking*, Burlington: Elsevier, Inc., 2007.
- [12] Nokia, *Nokia 22 Users Guide* [verkkodokumentti, viitattu 16.12.2009] saatavissa: [http://nds1.nokia.com/phones/files/guides/Nokia22\\_Users\\_Guide\\_en.pdf](http://nds1.nokia.com/phones/files/guides/Nokia22_Users_Guide_en.pdf).
- [13] Suositus, Viestintävirasto 309/2007, Hätäliikenteen ohjaus yritysverkosta [verkkodokumentti, viitattu 28.12.2009]. Saatavissa: <http://www.ficora.fi/attachments/suomiry/5pmZ2G6WH/Suositus3092007S.pdf>.
- [14] Casad, Joe – Willsey, Bob, *TCP/IP*, Helsinki: IT Press, 1999.

## SIP-VASTAUSKODIT [4;5;7]

1xx Informatiiviset	100	Yritetään	
	180	Hälyyttää	
	181	Puhelua ohjataan	
	182	Jonottaa	
	183	Istunto käynnissä	
2xx Onnistuminen	200	OK	
	202	Hyväksytty	
3xx Uudelleenohjaus	300	Useita vaihtoehtoja	
	301	Siirretty pysyvästi	
	302	Siirretty tilapäisesti	
	303	Etsi muualta	
	305	Käytä välityspalvelinta	
4xx Asiakasvirhe	380	Vaihtoehtoinen palvelu	
	400	Virheellinen pyyntö	
	401	Ei lupaa	
	402	Vaaditaan maksu	
	403	Piilotettu	
	404	Ei löydy	
	405	Metodia ei sallita	
	406	Ei hyväksyttävä	
	407	Välityspalvelimen todentaminen vaaditaan	
	408	Pyynnön aika loppui	
	409	Ristiriita	
	410	Puhelu menetetty	
	413	Pituus vaaditaan	
	414	Pyydetty URL liian suuri	
	415	Mediatyyppiä ei tueta	
	416	URI ei tuettu	
	420	Virheellinen alaliittymä	
	421	Alaliittymä vaaditaan	
	423	Väliaika liian lyhyt	
	480	Tilapäisesti ei käytettävissä	
	481	Puhelua tai tapahtumaa ei ole	
	482	Silmukka havaittu	
	483	Liian monta hyppyä	
	484	Osoite vaajaavainen	
	485	Moniselitteinen	
	486	Täällä ruuhkaa	
	487	Pyyntö purettu	
	488	Ei kelpaa täällä	
	489	Huono tapahtuma	
	491	Pyyntö odottaa	
	493	Selvittämätön	
	5xx Palvelin virheet	500	Sisäinen palvelin virhe
		501	Ei toteutettu
502		Virheellinen yhdyskäytävä	
503		Palvelu ei käytettävissä	
504		Yhdyskäytävän aika loppui	
505		SIP-versiota ei tueta	
6xx Globaalit virheet	513	Viesti liian pitkä	
	600	Kaikkialla ruuhkaa	
	603	Torjuminen	
	604	Ei esiinny missään	
	606	Ei hyväksyttävä	

**ERICSSON DIALOG 4422 IP:N KONFIGURAATIOTIEDOSTO**

*[system]*

*[Software]*

*BootFile=/dbc42x02/d42x02-boot\_R3L.dat*

*BootVersion=R3L*

*ApplicationFile=/dbc42x02/d42x02-applic\_R7E.dat*

*ApplicationVersion=R7E*

*[Absence]*

*Profile=\*10\*profileNo#, #10#*

*FollowMe=\*21\*extensionNo#, #21#*

*ExtFollowMe=\*22#extensionNo#, #22#*

*AbsenceReason=\*23\*reasonCode#, #23#*

*Vacation=6\*ddmm*

*DayOff=7\*ddmm*

*GoneHome=8\*hhmm*

*Illness=7\*ddmm*

*[Authorization]*

*Code=\*61\**

*Code=\*72\**

*Code=\*73\**

*Code=#73\**

*Code=\*74\**

*Code=\*75\*-\*n#*

*Code=\*76\**

*Code=#76\**

*[AutoNeg]*

*AutoNegLANPort=YES*

*AutoNegPCPort=YES*

*[Codecs]*

*G.711U*

*G.711A*

*[DebugLevel]*

*RTPDebug=2*

*SIPDebug=1*



*[DefaultPacketSize]*

*DefaultMsPerPacket711=30*

*DefaultMsPerPacket729=30*

*[DIFFSERVTCP]*

*TrafficClass=5*

*DropPrecedence=3*

*[DIFFSERVUDP]*

*TrafficClass=5*

*DropPrecedence=3*

*[Display]*

*ShowDTMFDigits=YES*

*ShowIPSettings=Enabled*

*[FunctionKeysDBC425]*

*CallBack=1*

*FollowMe=2*

*FreeOnSecond=3*

*MessageWaiting=5*

*Transfer=6*

*EnablePBXStoring=NO*

*[FunctionKeysDBC422]*

*Conference=0*

*Transfer=1*

*Settings=5*

*FollowMe=6*

*MessageWaiting=7*

*FreeOnSecond=8*

*CallList=9*

*EnablePBXStoring=NO*

*[FunctionKeysDBC420]*

*Conference=0*

*Transfer=1*

*FollowMe=6*

*MessageWaiting=7*

*FreeOnSecond=8*

*EnablePBXStoring=NO*

*[Handsfree]*

*[IPPhoneAdministrator]*

*IPPhoneAdministrator=YES*

*[Language]*

*LanguageFile=/dbc42x02/d42x02-lang\_R7C.txt*

*LanguageVersion=R7C*

*OptionalLanguage=EN,\*08\*0#*

*OptionalLanguage=FR,\*08\*1#*

*OptionalLanguage=DE,\*08\*2#*

*OptionalLanguage=ES,\*08\*3#*

*OptionalLanguage=IT,\*08\*4#*

*OptionalLanguage=SV,\*08\*5#*

*OptionalLanguage=FI,\*08\*6#*

*OptionalLanguage=DA,\*08\*7#*

*OptionalLanguage=NO,\*08\*8#*

*OptionalLanguage=NL,\*08\*9#*

*OptionalLanguage=PB,\*08\*9#*

*OptionalLanguage=SL,\*08\*9#*

*StartupLanguage=FI*

*[LEDs]*

*Cad0=185,5,5,5*

*Cad1=50,50,0,0*

*Cad2=30,30,0,0*

*[L2QOS]*

*PhonePort=0,0*

*PCPort=0,0*

*LANPort=0,0*

*BroadcastStormControlLimit=30 ;*

*[Password]*

*PasswordInputFormat=alphanumeric*

*PINorPassword=Password*

*ServiceCodeChangePIN=\*74\**

*[RingCads]*

*Internal=20,100,0,1,0,0 ;*

*External=7,6,7,100,0,0*

*Callback=6,8,56,8,0,0*

*Extra=6,8,6,8,6,8*

*Delay=7*

*[Security]*

*Security=DISABLED*

*CertificateValidate=NO*

*SecurityFallback=NO*

*SaveUserPassword=YES*

*SignallingEncrypted=NO*

*[SIP]*

*SIPDomain=80.221.63.205*

*SIPProxyAddress=80.221.63.205*

*SIPProxyPort=5060*

*SecureSIPProxyPort=5061*

*SIPUseTelURI=NO*

*SIPHookFlash=DTMF\_INFO\_!*

*SIP\_DTMF=INFO*

*[STOREPHONEBOOKS]*

*EnableStoring=NO*

*[SuffixServices]*

*Intrusion=6*

*CallWaiting=4*

*CallBack=5*

*CallPickUp=8*

*Conference=3*

*[Time]*

*TIMEZONE=CET:60:0:040101:110101*

*NTP-server=80.221.63.205*

*[Tones]*

*Dial tone=*

*0,0,*

*200,300,200,300,200,800,*

*425,-10,0,0,0,0,*

*0,0*

*Special dial tone=*

1,0,  
500,50,0,0,0,0,  
425,-10,0,0,0,0,  
0,0

*Busy tone=*

1,0,  
500,500,0,0,0,0,  
425,-10,0,0,0,0,  
0,0

*Alerting tone=*

1,0,  
1000,4000,0,0,0,0,  
425,-10,0,0,0,0,  
0,0

*Congestion tone=*

1,0,  
200,200,0,0,0,0,  
425,-10,0,0,0,0,  
0,0

*Special information tone=*

3,4,  
333,1,333,1,333,1000,  
950,-10,1400,-10,1800,-10,  
0,0

*Call waiting tone=*

2,0,  
200,600,200,3000,0,0,  
425,-10,0,0,0,0,  
0,0

*Offhook queuing tone=*

1,0,

2000,990,0,0,0,0,

1400,-10,0,0,0,0,

0,0

*On hold tone=*

2 ,1,

10,150,10,5000,0,0,

400,-10,300,-10,0,0,

0,0

*External dial tone=*

0,0,

500,0,0,0,0,0,

425,-10,0,0,0,0,

0,0

*Waiting voice tone=*

1,0,

30,330,0,0,0,0,

425,-10,0,0,0,0,

0,0

## CISCO SYSTEMS ATA 186-SOVITTIMEN ALOITUSKONFIGUROINTI

### DYNAAMISELLA IP-OSOITTEELLA:

1. Painetaan ATA-sovittimen punaista nappulaa, jolla käynnistetään konfigurointi tila.
2. Seuraavaksi puhelimesta kuullaan viesti "configuration menu, enter menu number".
3. Tyhjennetään ATA-sovittimen asetukset painelemalla phone1-liitäntään kytketystä puhelimesta "322873738#".
4. Seuraavaksi kuullaan puhelimesta viestin "to save press star(\*)...".
5. Tallennetaan muutokset painamalla puhelimesta \*-merkkiä, jonka jälkeen ATA-sovitin kysyy IP-osoitteen DHCP-palvelimelta.
6. Seuraavaksi selvitetään ATA-sovittimen uusi IP-osoite painelemalla puhelimesta "80#".
7. Lopuksi voidaan ottaa yhteys ATA-sovittimeen WWW-selaimella siirtymällä osoitteeseen <http://<ATA-laitteen IP-osoite>/dev> esim. <http://192.168.1.2/dev>

### STAATISELLA IP-OSOITEELLA:

1. Painetaan punaista nappulaa.
2. Otetaan DHCP-asetus pois päältä ATA-sovittimesta painelemalla DTMF-puhelimesta "20# 0# 3".
3. Asetetaan IP-osoite painelemalla "1#<1.oktetti>\* <2.oktetti> \* <3.oktetti> \* <4.oktetti> #3. Esim"1# 192\*168\*1\*2 #3".
4. Asetetaan aliverkkon peite painelemalla "10# 255\*255\*255\*0 3#".
5. Asetetaan oletus reititin (default gateway) painelemalla "28# 192\*168\*1\*1".
6. Laskettua luurin alas ja ATA-sovitin tallentaa uuden IP-osoitteen.

## CISCO SYSTEMS ATA 186-SOVITTIMEN KONFIGURAATIOT

UIPassword:	•	ToConfig:	0
UseTftp:	0	TftpURL:	80.221.54.142
CfgInterval:	3600	EncryptKey:	•
Dhcp:	1	StaticIP:	0.0.0.0
StaticRoute:	0.0.0.0	StaticNetMask:	0.0.0.0
UID0:	200	PWD0:	•••
UID1:	304	PWD1:	•••
GkOrProxy:	80.221.63.205	Gateway:	0
GateWay2:	0.0.0.0	UseLoginID:	0
LoginID0:	200	LoginID1:	304
AltGk:	0	AltGkTimeOut:	0
GkTimeToLive:	300	GkId:	.
UseSIP:	1	SIPRegInterval:	120
MaxRedirect:	8	SIPRegOn:	1
NATIP:	0.0.0.0	SIPPort:	5060
MediaPort:	16384	OutBoundProxy:	0
NatServer:	0	NatTimer:	0x00000000
LBRCCodec:	0	AudioMode:	0x00140014
RxCodec:	2	TxCodec:	2
NumTxFrames:	2	CallFeatures:	0xffffffff
PaidFeatures:	0xffffffff	CallerIdMethod:	0x00019e60
FeatureTimer:	0x00000000	Polarity:	0x00000000
ConnectMode:	0x00060400	AutMethod:	0x00000000
TimeZone:	2	NTPIP:	0.0.0.0
AltNTPIP:	0.0.0.0	DNS1IP:	0.0.0.0
DNS2IP:	0.0.0.0	TOS:	0x000068b8
SigTimer:	0x01418564	OpFlags:	0x00000002
VLANSetting:	0x0000002b	NPrintf:	0.0.0.0.0
TraceFlags:	0x00000000	RingOnOffTime:	2,4,25
IPDialPlan:	1	DialPlan:	*St4- #St4- 911 1>#t8.r
DialTone:	2,31538,30831,1380,15	BusyTone:	2,30467,28959,1191,15
ReorderTone:	2,30467,28959,1191,15	RingBackTone:	2,30831,30467,1943,25
CallWaitTone:	1,30831,0,5493,0,0,240	AlertTone:	1,30467,0,5970,0,0,480
CallCmd:	Af;AH;BS;NA;CS;NA;D		

**SIP-MERKINANTOVIESTIT SOITTAESSA OHJELMISTOPUHELIMESTA MATKAPUHELIMEEN**

<--- SIP read from 80.221.54.142:52934 --->  
 INVITE sip:00505247759@80.221.63.205 SIP/2.0  
 Via: SIP/2.0/UDP 80.221.54.142:52934;branch=z9hG4bK-d8754z-2225160ecf5fda58-1---d8754z-;rport  
 Max-Forwards: 70  
 Contact: <sip:300@80.221.54.142:52934>  
 To: "00505247759 (Softphone)"<sip:00505247759@80.221.63.205>  
 From: "mikko"<sip:300@80.221.63.205>;tag=581c3223  
 Call-ID: OTJmZjUzNzEyM2FIYjdkOWJmMTBjY2FIQGQ2YmIxNGY.  
 CSeq: 1 INVITE  
 Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO  
 Content-Type: application/sdp  
 User-Agent: X-Lite release 1103k stamp 53621  
 Content-Length: 265

v=0  
 o=- 2 2 IN IP4 80.221.54.142  
 s=CounterPath X-Lite 3.0  
 c=IN IP4 80.221.54.142  
 t=0 0  
 m=audio 3632 RTP/AVP 107 0 8 101  
 a=alt:1 1 : +WaShaO2 yMPNxvF8 80.221.54.142 3632  
 a=fmtp:101 0-15  
 a=rtpmap:107 BV32/16000  
 a=rtpmap:101 telephone-event/8000  
 a=sendrecv

<--- Reliably Transmitting (no NAT) to 80.221.54.142:52934 --->  
 SIP/2.0 407 Proxy Authentication Required  
 Via: SIP/2.0/UDP 80.221.54.142:52934;branch=z9hG4bK-d8754z-2225160ecf5fda58-1---d8754z-;received=80.221.54.142;rport=52934  
 From: "mikko"<sip:300@80.221.63.205>;tag=581c3223  
 To: "00505247759 (Softphone)"<sip:00505247759@80.221.63.205>;tag=as0e9c4931  
 Call-ID: OTJmZjUzNzEyM2FIYjdkOWJmMTBjY2FIQGQ2YmIxNGY.  
 CSeq: 1 INVITE  
 User-Agent: Asterisk PBX  
 Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY  
 Supported: replaces  
 Proxy-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="3cd6237c"  
 Content-Length: 0

<--- SIP read from 80.221.54.142:52934 --->  
 ACK sip:00505247759@80.221.63.205 SIP/2.0  
 Via: SIP/2.0/UDP 80.221.54.142:52934;branch=z9hG4bK-d8754z-2225160ecf5fda58-1---d8754z-;rport



To: "00505247759 (Softphone)"<sip:00505247759@80.221.63.205>;tag=as0e9c4931  
 From: "mikko"<sip:300@80.221.63.205>;tag=581c3223  
 Call-ID: OTJmZjUzNzEyM2FIYjdkOWJmMTBjY2FIOGQ2YmIxNGY.  
 CSeq: 1 ACK  
 Content-Length: 0

<--- SIP read from 80.221.54.142:52934 --->  
 INVITE sip:00505247759@80.221.63.205 SIP/2.0  
 Via: SIP/2.0/UDP 80.221.54.142:52934;branch=z9hG4bK-d8754z-a74bc00e604d1e57-1--  
 -d8754z-;rport  
 Max-Forwards: 70  
 Contact: <sip:300@80.221.54.142:52934>  
 To: "00505247759 (Softphone)"<sip:00505247759@80.221.63.205>  
 From: "mikko"<sip:300@80.221.63.205>;tag=581c3223  
 Call-ID: OTJmZjUzNzEyM2FIYjdkOWJmMTBjY2FIOGQ2YmIxNGY.  
 CSeq: 2 INVITE  
 Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE,  
 SUBSCRIBE, INFO  
 Content-Type: application/sdp  
 Proxy-Authorization: Digest user-  
 name="300",realm="asterisk",nonce="3cd6237c",uri="sip:00505247759@80.221.63.205",  
 response="482e4af8e1570c3f08d877ee4871fb34",algorithm=MD5  
 User-Agent: X-Lite release 1103k stamp 53621  
 Content-Length: 265

v=0  
 o=- 2 2 IN IP4 80.221.54.142  
 s=CounterPath X-Lite 3.0  
 c=IN IP4 80.221.54.142  
 t=0 0  
 m=audio 3632 RTP/AVP 107 0 8 101  
 a=alt:1 1 : +WaShaO2 yMPNxvF8 80.221.54.142 3632  
 a=fmtp:101 0-15  
 a=rtpmap:107 BV32/16000  
 a=rtpmap:101 telephone-event/8000  
 a=sendrecv

<--- Transmitting (no NAT) to 80.221.54.142:52934 --->  
 SIP/2.0 100 Trying  
 Via: SIP/2.0/UDP 80.221.54.142:52934;branch=z9hG4bK-d8754z-a74bc00e604d1e57-1--  
 -d8754z-;received=80.221.54.142;rport=52934  
 From: "mikko"<sip:300@80.221.63.205>;tag=581c3223  
 To: "00505247759 (Softphone)"<sip:00505247759@80.221.63.205>  
 Call-ID: OTJmZjUzNzEyM2FIYjdkOWJmMTBjY2FIOGQ2YmIxNGY.  
 CSeq: 2 INVITE  
 User-Agent: Asterisk PBX  
 Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY  
 Supported: replaces  
 Contact: <sip:00505247759@80.221.63.205>  
 Content-Length: 0

&lt;-----&gt;

Reliably Transmitting (no NAT) to 80.221.48.197:5060:  
 INVITE sip:304@80.221.48.197:5060;user=phone;transport=udp SIP/2.0  
 Via: SIP/2.0/UDP 80.221.63.205:5060;branch=z9hG4bK5baf6379;rport  
 From: "mikko" <sip:300@80.221.63.205>;tag=as3075f158  
 To: <sip:304@80.221.48.197:5060;user=phone;transport=udp>  
 Contact: <sip:300@80.221.63.205>  
 Call-ID: 57e8f8da5cf0d2ae0622f99b24b919f2@80.221.63.205  
 CSeq: 102 INVITE  
 User-Agent: Asterisk PBX  
 Max-Forwards: 70  
 Date: Thu, 07 Jan 2010 01:55:41 GMT  
 Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY  
 Supported: replaces  
 Content-Type: application/sdp  
 Content-Length: 240

v=0  
 o=root 2687 2687 IN IP4 80.221.63.205  
 s=session  
 c=IN IP4 80.221.63.205  
 t=0 0  
 m=audio 14532 RTP/AVP 0 101  
 a=rtpmap:0 PCMU/8000  
 a=rtpmap:101 telephone-event/8000  
 a=fmtp:101 0-16  
 a=silenceSupp:off - - - -  
 a=ptime:20  
 a=sendrecv

<--- Transmitting (no NAT) to 80.221.54.142:52934 --->  
 SIP/2.0 180 Ringing  
 Via: SIP/2.0/UDP 80.221.54.142:52934;branch=z9hG4bK-d8754z-a74bc00e604d1e57-1--  
 -d8754z-;received=80.221.54.142;rport=52934  
 From: "mikko" <sip:300@80.221.63.205>;tag=581c3223  
 To: "00505247759 (Softphone)" <sip:00505247759@80.221.63.205>;tag=as1d57e77b  
 Call-ID: OTJmZjUzNzEyM2FIYjdkOWJmMTBjY2FIOGQ2YmIxNGY.  
 CSeq: 2 INVITE  
 User-Agent: Asterisk PBX  
 Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY  
 Supported: replaces  
 Contact: <sip:00505247759@80.221.63.205>  
 Content-Length: 0

<--- SIP read from 80.221.48.197:5060 --->  
 SIP/2.0 100 Trying  
 Via: SIP/2.0/UDP 80.221.63.205:5060;branch=z9hG4bK5baf6379;rport  
 From: "mikko" <sip:300@80.221.63.205>;tag=as3075f158  
 To: <sip:304@80.221.48.197:5060;user=phone;transport=udp>;tag=3150794108

Call-ID: 57e8f8da5cf0d2ae0622f99b24b919f2@80.221.63.205  
CSeq: 102 INVITE  
Server: Cisco ATA 186 v2.16.1 ata18x (030709a)  
Content-Length: 0

<--- SIP read from 80.221.48.197:5060 --->

SIP/2.0 180 Ringing  
Via: SIP/2.0/UDP 80.221.63.205:5060;branch=z9hG4bK5baf6379;rport  
From: "mikko" <sip:300@80.221.63.205>;tag=as3075f158  
To: <sip:304@80.221.48.197:5060;user=phone;transport=udp>;tag=3150794108  
Call-ID: 57e8f8da5cf0d2ae0622f99b24b919f2@80.221.63.205  
CSeq: 102 INVITE  
Server: Cisco ATA 186 v2.16.1 ata18x (030709a)  
Content-Length: 0

<--- SIP read from 80.221.48.197:5060 --->

SIP/2.0 200 OK  
Via: SIP/2.0/UDP 80.221.63.205:5060;branch=z9hG4bK5baf6379;rport  
From: "mikko" <sip:300@80.221.63.205>;tag=as3075f158  
To: <sip:304@80.221.48.197:5060;user=phone;transport=udp>;tag=3150794108  
Call-ID: 57e8f8da5cf0d2ae0622f99b24b919f2@80.221.63.205  
CSeq: 102 INVITE  
Contact: <sip:304@80.221.48.197:5060;user=phone;transport=udp>  
Server: Cisco ATA 186 v2.16.1 ata18x (030709a)  
Content-Length: 192  
Content-Type: application/sdp

v=0  
o=304 204 204 IN IP4 80.221.48.197  
s=ATA186 Call  
c=IN IP4 80.221.48.197  
t=0 0  
m=audio 16386 RTP/AVP 0 101  
a=rtpmap:0 PCMU/8000/1  
a=rtpmap:101 telephone-event/8000  
a=fmtp:101 0-15

<----->

Transmitting (no NAT) to 80.221.48.197:5060:  
ACK sip:304@80.221.48.197:5060;user=phone;transport=udp SIP/2.0  
Via: SIP/2.0/UDP 80.221.63.205:5060;branch=z9hG4bK34f63222;rport  
From: "mikko" <sip:300@80.221.63.205>;tag=as3075f158  
To: <sip:304@80.221.48.197:5060;user=phone;transport=udp>;tag=3150794108  
Contact: <sip:300@80.221.63.205>  
Call-ID: 57e8f8da5cf0d2ae0622f99b24b919f2@80.221.63.205  
CSeq: 102 ACK  
User-Agent: Asterisk PBX  
Max-Forwards: 70  
Content-Length: 0

<--- Reliably Transmitting (no NAT) to 80.221.54.142:52934 --->  
 SIP/2.0 200 OK  
 Via: SIP/2.0/UDP 80.221.54.142:52934;branch=z9hG4bK-d8754z-a74bc00e604d1e57-1--  
 -d8754z-;received=80.221.54.142;rport=52934  
 From: "mikko" <sip:300@80.221.63.205>;tag=581c3223  
 To: "00505247759 (Softphone)" <sip:00505247759@80.221.63.205>;tag=as1d57e77b  
 Call-ID: OTJmZjUzNzEyM2FIYjdkOWJmMTBjY2FIOGQ2YmIxNGY.  
 CSeq: 2 INVITE  
 User-Agent: Asterisk PBX  
 Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY  
 Supported: replaces  
 Contact: <sip:00505247759@80.221.63.205>  
 Content-Type: application/sdp  
 Content-Length: 240

v=0  
 o=root 2687 2687 IN IP4 80.221.63.205  
 s=session  
 c=IN IP4 80.221.63.205  
 t=0 0  
 m=audio 11300 RTP/AVP 0 101  
 a=rtpmap:0 PCMU/8000  
 a=rtpmap:101 telephone-event/8000  
 a=fmtp:101 0-16  
 a=silenceSupp:off - - - -  
 a=ptime:20  
 a=sendrecv

<--- SIP read from 80.221.54.142:52934 --->  
 ACK sip:00505247759@80.221.63.205 SIP/2.0  
 Via: SIP/2.0/UDP 80.221.54.142:52934;branch=z9hG4bK-d8754z-5e6dee42aa45db39-1--  
 -d8754z-;rport  
 Max-Forwards: 70  
 Contact: <sip:300@80.221.54.142:52934>  
 To: "00505247759 (Softphone)" <sip:00505247759@80.221.63.205>;tag=as1d57e77b  
 From: "mikko" <sip:300@80.221.63.205>;tag=581c3223  
 Call-ID: OTJmZjUzNzEyM2FIYjdkOWJmMTBjY2FIOGQ2YmIxNGY.  
 CSeq: 2 ACK  
 Proxy-Authorization: Digest user-  
 name="300",realm="asterisk",nonce="3cd6237c",uri="sip:00505247759@80.221.63.205",  
 response="482e4af8e1570c3f08d877ee4871fb34",algorithm=MD5  
 User-Agent: X-Lite release 1103k stamp 53621  
 Content-Length: 0  
 <----->

Reliably Transmitting (no NAT) to 80.221.48.197:5060:  
 OPTIONS sip:200@80.221.48.197:5060;user=phone;transport=udp SIP/2.0  
 Via: SIP/2.0/UDP 80.221.63.205:5060;branch=z9hG4bK56271a94;rport  
 From: "asterisk" <sip:asterisk@80.221.63.205>;tag=as03668672  
 To: <sip:200@80.221.48.197:5060;user=phone;transport=udp>

Contact: <sip:asterisk@80.221.63.205>  
 Call-ID: 63d8ce837a5cc598145b8df17a55bd21@80.221.63.205  
 CSeq: 102 OPTIONS  
 User-Agent: Asterisk PBX  
 Max-Forwards: 70  
 Date: Thu, 07 Jan 2010 01:55:48 GMT  
 Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY  
 Supported: replaces  
 Content-Length: 0

<--- SIP read from 80.221.48.197:5060 --->  
 SIP/2.0 200 OK  
 Via: SIP/2.0/UDP 80.221.63.205:5060;branch=z9hG4bK56271a94;rport  
 From: "asterisk" <sip:asterisk@80.221.63.205>;tag=as03668672  
 To: <sip:200@80.221.48.197:5060;user=phone;transport=udp>;tag=371020734  
 Call-ID: 63d8ce837a5cc598145b8df17a55bd21@80.221.63.205  
 CSeq: 102 OPTIONS  
 Server: Cisco ATA 186 v2.16.1 ata18x (030709a)  
 Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER  
 Content-Length: 244  
 Content-Type: application/sdp

v=0  
 o=200 823 823 IN IP4 80.221.48.197  
 s=ATA186 Call  
 c=IN IP4 80.221.48.197  
 t=0 0  
 m=audio 16384 RTP/AVP 0 8 4 101  
 a=rtpmap:0 PCMU/8000/1  
 a=rtpmap:8 PCMA/8000/1  
 a=rtpmap:4 G723/8000/1  
 a=rtpmap:101 telephone-event/8000  
 a=fmtp:101 0-15

<----->  
 <--- SIP read from 80.221.48.197:5060 --->  
 BYE sip:300@80.221.63.205 SIP/2.0  
 Via: SIP/2.0/UDP 80.221.48.197:5060  
 From: <sip:304@80.221.48.197;user=phone;transport=udp>;tag=3150794108  
 To: "mikko" <sip:300@80.221.63.205>;tag=as3075f158  
 Call-ID: 57e8f8da5cf0d2ae0622f99b24b919f2@80.221.63.205  
 CSeq: 1 BYE  
 User-Agent: Cisco ATA 186 v2.16.1 ata18x (030709a)  
 Content-Length: 0

<--- Transmitting (no NAT) to 80.221.48.197:5060 --->  
 SIP/2.0 200 OK  
 Via: SIP/2.0/UDP 80.221.48.197:5060;received=80.221.48.197  
 From: <sip:304@80.221.48.197;user=phone;transport=udp>;tag=3150794108  
 To: "mikko" <sip:300@80.221.63.205>;tag=as3075f158

Call-ID: 57e8f8da5cf0d2ae0622f99b24b919f2@80.221.63.205  
CSeq: 1 BYE  
User-Agent: Asterisk PBX  
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY  
Supported: replaces  
Content-Length: 0

<----->

Reliably Transmitting (no NAT) to 80.221.54.142:52934:  
BYE sip:300@80.221.54.142:52934 SIP/2.0  
Via: SIP/2.0/UDP 80.221.63.205:5060;branch=z9hG4bK1985875d;rport  
From: "00505247759 (Softphone)"<sip:00505247759@80.221.63.205>;tag=as1d57e77b  
To: "mikko"<sip:300@80.221.63.205>;tag=581c3223  
Call-ID: OTJmZjUzNzEyM2FIYjdkOWJmMTBjY2FIOGQ2YmIxNGY.  
CSeq: 102 BYE  
User-Agent: Asterisk PBX  
Max-Forwards: 70  
X-Asterisk-HangupCause: Normal Clearing  
X-Asterisk-HangupCauseCode: 16  
Content-Length: 0

<--- SIP read from 80.221.54.142:52934 --->

SIP/2.0 200 OK  
Via: SIP/2.0/UDP 80.221.63.205:5060;branch=z9hG4bK1985875d;rport=5060  
Contact: <sip:300@80.221.54.142:52934>  
To: "mikko"<sip:300@80.221.63.205>;tag=581c3223  
From: "00505247759 (Softphone)"<sip:00505247759@80.221.63.205>;tag=as1d57e77b  
Call-ID: OTJmZjUzNzEyM2FIYjdkOWJmMTBjY2FIOGQ2YmIxNGY.  
CSeq: 102 BYE  
User-Agent: X-Lite release 1103k stamp 53621  
Content-Length: 0

<--- SIP read from 80.221.48.197:5060 --->

REGISTER sip:80.221.63.205 SIP/2.0  
Via: SIP/2.0/UDP 80.221.48.197:5060  
From: <sip:304@80.221.63.205;user=phone>;tag=234013826  
To: <sip:304@80.221.63.205;user=phone>  
Call-ID: 3673236243@80.221.48.197  
CSeq: 6110 REGISTER  
Contact: <sip:304@80.221.48.197:5060;user=phone;transport=udp>;expires=120  
User-Agent: Cisco ATA 186 v2.16.1 ata18x (030709a)  
Content-Length: 0

<--- Transmitting (no NAT) to 80.221.48.197:5060 --->

SIP/2.0 100 Trying  
Via: SIP/2.0/UDP 80.221.48.197:5060;received=80.221.48.197  
From: <sip:304@80.221.63.205;user=phone>;tag=234013826  
To: <sip:304@80.221.63.205;user=phone>  
Call-ID: 3673236243@80.221.48.197  
CSeq: 6110 REGISTER

User-Agent: Asterisk PBX  
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY  
Supported: replaces  
Content-Length: 0

<--- Transmitting (no NAT) to 80.221.48.197:5060 --->

SIP/2.0 200 OK

Via: SIP/2.0/UDP 80.221.48.197:5060;received=80.221.48.197

From: <sip:304@80.221.63.205;user=phone>;tag=234013826

To: <sip:304@80.221.63.205;user=phone>;tag=as527ef4ae

Call-ID: 3673236243@80.221.48.197

CSeq: 6110 REGISTER

User-Agent: Asterisk PBX

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY

Supported: replaces

Expires: 120

Contact: <sip:304@80.221.48.197:5060;user=phone;transport=udp>;expires=120

Date: Thu, 07 Jan 2010 01:56:13 GMT

Content-Length: 0

<--- SIP read from 80.221.48.197:5060 --->

REGISTER sip:80.221.63.205 SIP/2.0

Via: SIP/2.0/UDP 80.221.48.197:5060

From: <sip:200@80.221.63.205;user=phone>;tag=2321746024

To: <sip:200@80.221.63.205;user=phone>

Call-ID: 3349830766@80.221.48.197

CSeq: 6110 REGISTER

Contact: <sip:200@80.221.48.197:5060;user=phone;transport=udp>;expires=120

User-Agent: Cisco ATA 186 v2.16.1 ata18x (030709a)

Content-Length: 0

<--- Transmitting (no NAT) to 80.221.48.197:5060 --->

SIP/2.0 100 Trying

Via: SIP/2.0/UDP 80.221.48.197:5060;received=80.221.48.197

From: <sip:200@80.221.63.205;user=phone>;tag=2321746024

To: <sip:200@80.221.63.205;user=phone>

Call-ID: 3349830766@80.221.48.197

CSeq: 6110 REGISTER

User-Agent: Asterisk PBX

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY

Supported: replaces

Content-Length: 0

<----->

Reliably Transmitting (no NAT) to 80.221.48.197:5060:

OPTIONS sip:200@80.221.48.197:5060;user=phone;transport=udp SIP/2.0

Via: SIP/2.0/UDP 80.221.63.205:5060;branch=z9hG4bK5190d8c0;rport

From: "asterisk" <sip:asterisk@80.221.63.205>;tag=as12ba139e

To: <sip:200@80.221.48.197:5060;user=phone;transport=udp>

Contact: <sip:asterisk@80.221.63.205>

Call-ID: 20568b8c3f4ba1b417a0b503282733d4@80.221.63.205  
CSeq: 102 OPTIONS  
User-Agent: Asterisk PBX  
Max-Forwards: 70  
Date: Thu, 07 Jan 2010 01:56:28 GMT  
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY  
Supported: replaces  
Content-Length: 0

<--- Transmitting (no NAT) to 80.221.48.197:5060 --->

SIP/2.0 200 OK  
Via: SIP/2.0/UDP 80.221.48.197:5060;received=80.221.48.197  
From: <sip:200@80.221.63.205;user=phone>;tag=2321746024  
To: <sip:200@80.221.63.205;user=phone>;tag=as22af2334  
Call-ID: 3349830766@80.221.48.197  
CSeq: 6110 REGISTER  
User-Agent: Asterisk PBX  
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY  
Supported: replaces  
Expires: 120  
Contact: <sip:200@80.221.48.197:5060;user=phone;transport=udp>;expires=120  
Date: Thu, 07 Jan 2010 01:56:28 GMT  
Content-Length: 0

<--- SIP read from 80.221.48.197:5060 --->

SIP/2.0 200 OK  
Via: SIP/2.0/UDP 80.221.63.205:5060;branch=z9hG4bK5190d8c0;rport  
From: "asterisk" <sip:asterisk@80.221.63.205>;tag=as12ba139e  
To: <sip:200@80.221.48.197:5060;user=phone;transport=udp>;tag=371020734  
Call-ID: 20568b8c3f4ba1b417a0b503282733d4@80.221.63.205  
CSeq: 102 OPTIONS  
Server: Cisco ATA 186 v2.16.1 ata18x (030709a)  
Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER  
Content-Length: 246  
Content-Type: application/sdp

v=0  
o=200 4850 4850 IN IP4 80.221.48.197  
s=ATA186 Call  
c=IN IP4 80.221.48.197  
t=0 0  
m=audio 16384 RTP/AVP 0 8 4 101  
a=rtpmap:0 PCMU/8000/1  
a=rtpmap:8 PCMA/8000/1  
a=rtpmap:4 G723/8000/1  
a=rtpmap:101 telephone-event/8000  
a=fmtp:101 0-15