



TEKNILLINEN KORKEAKOULU  
Sähkö- ja tietoliikennetekniikan osasto  
Teletekniikan laboratorio

S-38.128 Teletekniikan erikoistyö

# Session Initiation Protocol (SIP)

Tekijä:	Jutta Kaikkonen, 42890J
Ohjaaja:	Vesa Kosonen
Jätetty:	15.11.1999

## Tiivistelmä

Tämän erikoistyön tavoitteena on antaa lukijalle yleiskäsitys SIP-protokollasta (Session Initiation Protocol). SIP on suhteellisen uusi IETF:n suositus, joka määrittelee signaloinnin IP-puheluille. IP-puhelutekniikka on kasvattanut merkitystään viime vuosina ja sen uskotaan kasvavan perinteisen puhelinverkon kilpailijaksi muutaman vuoden kuluessa. SIP on yksinkertainen tekstipohjainen protokolla, jonka avulla voi toteuttaa lähes kaikki nykyisten puhelinverkkojen palvelut ja monia uudentyyppisiä palveluita kuten kolmannen osapuolen puhelunohjaus ja puhelukutsuparametrit. SIPin kilpailija, ITU.T:n suositus H.323, on osittain ehtinyt jo valtaamaan IP-puhelumarkkinat ja SIPin kannattajilla tulee olemaan erittäin raskas työ todistaa laitevalmistajille protokollan olevan toteutuksen arvoinen. Vasta tulevaisuus näyttää mikä protokolla vie voiton IP-puhelukisassa.

## Sisällysluettelo

<b>TIIVISTELMÄ</b> .....	<b>1</b>
<b>SISÄLLYSLUETTELO</b> .....	<b>2</b>
<b>LYHENTEET</b> .....	<b>4</b>
<b>1 JOHDANTO</b> .....	<b>5</b>
<b>2 YLEISTÄ</b> .....	<b>5</b>
2.1 PUHELUT IP-VERKOSSA .....	5
<b>3 KEHITYS</b> .....	<b>6</b>
<b>4 SIP PROTOKOLLA</b> .....	<b>8</b>
4.1 YMPÄRÖIVÄT PROTOKOLLAT .....	9
4.1.1 IP (RFC 791).....	9
4.1.2 TCP (RFC 793).....	9
4.1.3 UDP (RFC 768).....	10
4.1.4 RTP (RFC 1889).....	10
4.1.5 RTCP (RFC 1889).....	10
4.1.6 RSVP (RFC 2205).....	10
4.1.7 RTSP (RFC 2326).....	11
4.1.8 SDP (RFC 2327).....	11
4.1.9 SAP (Internet draft).....	11
4.2 SIP-KOMPONENTIT .....	11
4.2.1 Käyttäjäagentti .....	11
4.2.2 Välityspalvelin .....	12
4.2.3 Uudelleensuuntauspalvelin .....	12
4.3 SIP-OSOITTEET .....	12
4.4 SIP-SANOMAT .....	13
4.4.1 Otsikkokentät .....	13
4.4.2 Pyynnöt .....	15
4.4.3 Vastaukset.....	16
4.5 ESIMERKKI SIP-SANOMIEN KULUSTA .....	17
4.5.1 Välityspalvelimen käyttö.....	17
4.5.2 Uudelleensuuntauspalvelimen käyttö .....	18
4.6 TURVALLISUUSNÄKÖKOHDAT SIP:SSÄ.....	19
<b>5 SIPIN TARJOAMAT PALVELUT</b> .....	<b>20</b>
5.1 KÄYTTÄJÄN LIIKKUVUUS .....	22
<b>6 MUUT VOIP-STANDARDIT</b> .....	<b>24</b>
6.1 H.323 .....	24
6.2 SIP:N JA H.323:N VERTAILU.....	26
6.2.1 Toiminnan yksinkertaisuus.....	26
6.2.2 Kyvykkyystietojen vaihto (capability exchange).....	27
6.2.3 Toiminnallisuuden laajennettavuus.....	27
6.2.4 Yhteensopivuus muiden signaalointiprotokollien kanssa.....	27
6.2.5 Toteutuksen yksinkertaisuus.....	28
6.2.6 Vikasietoisuus .....	28
6.2.7 Kolmannen osapuolen ohjaus.....	28
<b>7 SIP TUOTTEET MARKKINOILLA</b> .....	<b>28</b>

Session Initiation Protocol (SIP)

<b>8</b>	<b>TULEVAISUUS .....</b>	<b>29</b>
	<b>VIITTEET .....</b>	<b>31</b>

## Lyhenteet

ASN.1	Abstract Syntax Notation One
B-ISDN	Broadband Integrated Services Data Network
HTTP	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
IIS	Internet Integrated Service
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPSEC	Internet Protocol Security Achitecture
ISDN	Integrated Services Data Network
ISO	International Standards Organization
ITU-T	International Telecommunications Union - Telecommunications Standardization Sector
MC	Multipoint Controller
MCU	Multipoint Control Unit
MP	Multipoint Processor
MMUSIC	Multiparty Multimedia Session Control
OSI	Open Systems Interconnection
PC	Personal Computer
PGP	Pretty Good Privacy
PER	Packet Encoding Rules
POP	Post Office Protocol
PSTN	Public Switched Telephone Network
RFC	Request For Comments
RSVP	Resource Reservation Protocol
RTCP	RTP Control Protocol
RTP	Real time Transport Protocol
RTSP	Real Time Streaming Protocol
SAP	Session Announcement Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Universal Resource Locator
UTF-8	Universal Character Set Transformation Format 8
VoIP	Voice over IP
VPN	Virtual Private Network
WWW	World Wide Web

## 1 Johdanto

Tämän erikoistyön tavoitteena on esitellä IP-puhelujen välitykseen käytettävä protokolla nimeltä Session Initiation Protocol (SIP). Työssä esitellään SIP-protokolla pääpiirteittäin, sen tarjoamat palvelut ja mahdolliset käyttötavat sekä verrataan SIPiä muihin IP-puhelusuosituksiin, lähinnä ITU-T:n H.323:een. H.323 esitellään hyvin lyhyesti.

Työn pohjana on pitkälti käytetty IETF:n RFC 2543:a, jossa SIP-protokolla on määritelty. Lisäksi on tutkittu aiheeseen liittyviä (lähinnä Internetistä löytyviä) artikkeleja, julkaisuja ja suosituksia.

## 2 Yleistä

### 2.1 Puhelut IP-verkossa

IP-verkkoja, Internettiä, on perinteisesti käytetty lähinnä tietokoneiden välisen teksti- tai kuvatedon välitykseen. Sen kautta on lähetetty sähköpostisanomia, luettu WWW-sivuja ja siirretty tiedostoja. IP-verkossa voidaan kuitenkin siirtää mitä tahansa digitaalisessa muodossa olevaa dataa, myös ääntä tai liikkuvaa kuvaa. IP-verkkojen jatkuva kasvu ja liikenteen eksponentiaalinen lisääntyminen on herättänyt niin palveluntarjoajat kuin laitevalmistajatkin mukaan kehittämään uusia käyttötapoja tälle medialle. Ensimmäisenä näistä uusista palveluista on markkinoille tulleet IP-puhelut. Teknologian ja markkinoiden kypsyttyä myös muita IP-verkkoja hyödyntäviä palveluita tullaan esittelemään, kuten videokonferenssi- ja etätyöskentelyjärjestelmiä sekä virtuaalisia yksityisverkkoja (Virtual Private Networks, VPN).

IP-puheluissa Internettiä (tai internettiä - tarkoittaen mitä tahansa IP-protokollalla toimivaa verkkoa, myös erillään maailmanlaajuisesta Internetistä olevaa) käytetään siirtämään digitoitua puhetta kahden tai useamman käyttäjän välillä reaaliaikaisesti. IP-puheluissa käytettiin alunperin terminaalina mikrofoni ja kaiuttimella varustettua multimedia-PC:tä, nykyisin yhä useammin tavallista puhelinta.

IP-puhelut ovat kehittyneet 1990-luvun puolivälistä lähtien nopealla vauhdilla ja nykyinen tekniikka mahdollistaa jo suhteellisen helposti keskustelun käymisen IP-verkon läpi. Kehitys on

edelleenkin kiihtyvää ja lähes jokainen tietoliikennealan yritys nykyään panostaa tämän aihealueen tutkimiseen ja kehittämiseen.

Tällä hetkellä IP-puhelut toimivat kuitenkin lähinnä suljetuissa ja kontrolloiduissa IP-verkoissa eli intraneteissa. Julkisessa, kaikille avoimessa Internetissä puheysteitä kahden tietokoneen välillä ei vielä aina pystytä takaamaan johtuen Internet-liikennepalvelun "best-effort"-luonteesta, palvelunlaadun ennustamattomuudesta ja suuresta viivevaihtelusta. Tästä syystä puhutaan mieluummin IP-puheluista kuin Internetpuheluista. Tämä ei kuitenkaan tarkoita sitä, ettei julkista Internetiä tulisi koskaan käyttämään puheluiden välitykseen - päin vastoin: kaikille avoimen Internetin etuna on sen maailmanlaajuiset ulottuvuudet ja rajoittamattomat laajenemismahdollisuudet.

IP-puhelujen signalointiin ja hallintaan on kehitetty kaksi kilpailevaa protokollaa. Laajemmin näistä on käytössä H.323, joka on ITU-T:n (International Telecommunication Union – Telecommunication Sector) suositus. Uudempi tulokas on IETF:n (Internet Engineering Task Force) suositus SIP eli Session Initiation Protocol. Nämä suositukset lähestyvät samaa ongelmaa hyvin erilaiselta näkökannalta: H.323 pohjaa ITU-T:n aiempiin standardeihin kuten ISDN-signaaloinnin Q.931:een ja aiempiin H-sarjan suosituksiin, kun taas SIP edustaa huomattavasti kevyempää Internet-maailman lähetyntapaa ja pohjautuu jossain määrin muun muassa HTTP:hen (HyperText Transfer Protocol).

### **3 Kehitys**

IP-puhelujen kehityksen kuvaus on syytä aloittaa IP-verkkojen kaupallistumisen ensivaiheista, 1990-luvun alkuvuosista. Vuonna 1991 siihen asti akateemisessa ja sotilaallisessa käytössä olleeseen Internetiin päästettiin ensimmäiset kaupalliset käyttäjät ja vuonna 1993 syntyi ensimmäinen jokakodin Internetpalvelu, WWW eli World Wide Web. Tämä toi Internetin miljoonien ihmisten ulottuville ja mahdollisti erilaisten massoille tarkoitettujen palvelujen tarjoamisen.

IP-puheluiden markkinat ovat siirtyneet muutamassa vuodessa harrasteluvaiheesta hintatietoisia kuluttajia ja yrityksiä houkuttelevaksi edulliseksi vaihtoehdoksi. Tämän vuoden alkupuoliskolla esiteltiin järjestelmiä, jotka tuovat käyttäjälle palveluita joita perinteisistä puhelimista ei löydy ja

jotka tekevät IP-puhelun käyttämisen soittajalle näkymättömäksi. Näiden myötä IP-puhelut tulevat mitä todennäköisimmin yhä suuremman käyttäjäkunnan ulottuville.

Kaikki alkoi kuitenkin vain muutama vuosi sitten: Vuoden 1995 loppupuolella muutamat harrastelijat huomasivat Internetin tarjoamat mahdollisuudet puheluiden välittämiseen. Yritykset kuten VocalTec, NetSpeak ja Quarterdeck kehittivät ohjelmia, joiden avulla kaksi Internetkäyttäjää saattoi keskustella toistensa kanssa. Edellytyksenä oli se, että kummassakin PC:ssä oli äänikortit, nopeat modeemit ja ennen kaikkea standardien puuttuessa samanlaiset IP-puheluohjelmistot. (Mine 1998)

Alkuaikoinaan IP-puheluita käytettiin kuten keskustelupalveluita ja puheluohjelmistojen kehittäjät pystyttivät käyttäjilleen foorumeja joissa saman ohjelmiston käyttäjät voivat löytää toisensa ja sopia esimerkiksi yksityisistä keskusteluista.

Hintatietoisten kuluttajien vaihe alkoi kun varhaiset käyttäjät äkkiä ymmärsivät, että IP-puheluiden läpilyönti riippui siitä kuinka hyvin niiden avulla voitiin kiertää viranomaisten sääntelyä ja tariffimääräyksiä. Varsinkin Yhdysvalloissa kaukopuhelujen markkinoilla on suuri hintajousto eli asiakkaat reagoivat hinnanalennuksiin lisäämällä puhelujaan huomattavasti ja päinvastoin. Tästä syystä kaukopuheluoperaattorit tunnistivat IP-puhelut suureksi uhaksi silloiselle toiminnalleen ja monet heistä lähtivät mukaan teknologian kehittämiseen pystyäkseen vastamaan sen tuomiin haasteisiin.

Samaan aikaan ohjelmistovalmistajat kuten VocalTec, Vienna Systems ja Clarent Corp huomasivat että huolimatta harrastelijamarkkinoissa saavutetusta hyvästä alusta, todellinen tavoite oli valloittaa tavalliset puhelinlaitteet: multimedia-PC:iden käyttäjäkunta on kuitenkin minimaalinen verrattuna puhelinten käyttäjien potentiaaliin markkinoihin. Lisäksi puheen laatu, joka oli IP-puhelujen suurin ongelma, riippui usein suuresti harrastelijoiden kyvystä konfiguroida PC-järjestelmänsä. Kommunikointi puhelimesta puhelimeen ja PC:stä puhelimeen tarjosi lupaavat markkinat ja toi mukanaan seuraavan sukupolven IP-puhelualustan, gatewayn eli yhdyskäytävän.

Gateway on laite, jonka avulla tavallisesta puhelinlaitteesta voi soittaa IP-puheluja. Se toimii yhdyskäytävänä puhelinverkon ja IP-verkon välillä eli paketoit puhelinverkosta tulevat signaalit IP-verkkoon, vastaanottajan päässä purkaa paketit ja lähettää signaalin edelleen puhelinverkkoon.

Yritysten houkuttelevuus IP-puheluiden käyttäjiksi ei ole ollut aivan yhtä helppoa kuin kuluttajien. Niillä on usein valmiit puhelinverkot ja niiden vaihtamiseen tarvittaisiin erittäin päteviä syitä. Yritysten innostusta on toistaiseksi hidastanut myös kunnollisten yrityksille suunnattujen pakettiratkaisujen puute, epäilykset palveluiden laadun tasosta ja tarjolla olevien laitteiden ja ohjelmistojen kypsyyttömyys ja liiankin nopea kehitys.

Viimeisen vuoden aikana yritykset kuten VegaStream ovat tuoneet markkinoille laitteita joiden avulla asiakas voi soittaa IP-puheluita täysin samalla tavalla kuin tavallisen puhelinverkon kautta. Kaiken todennäköisyyden mukaan IP-puhelujen yleistymisen jokakodin tiedonvälityskanavaksi on jo erittäin lähellä.

## 4 SIP protokolla

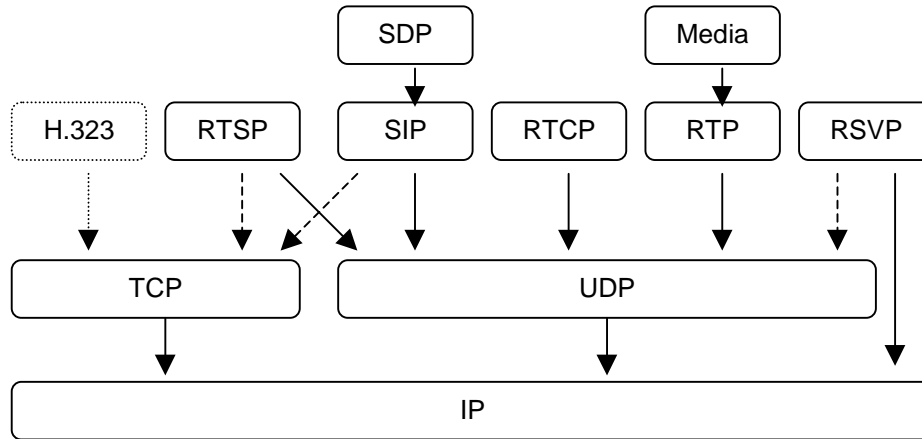
Session Initiation Protocol (SIP) on sovellustason protokolla, jolla voidaan muodostaa, muuttaa ja katkaista multimediayhteyksiä tai -puheluita. Multimediayhteykset voivat olla esimerkiksi puhelin- tai videoneuvotteluja, etäopiskelua tai Internetpuheluita.

SIP sai alkunsa IETF:n MMUSIC (Multiparty Multimedia Session Control) työryhmässä. Se on itse asiassa vain yksi jäsen IETF:n IP-puheluprotokollaperheessä. IETF:n multimedia-arkkitehtuuriin voidaan katsoa kuuluvan SIP:n lisäksi viisi muuta protokollaa:

- Real Time Streaming Protocol (RTSP), joka kontrolloi datavirran kulkua,
- Resource Reservation Protocol (RSVP), jonka avulla varataan verkkokapasiteettia,
- Real-time Transport Protocol (RTP), jolla kuljetetaan reaaliaikaista dataa internetissä
- RTP Control Protocol (RTCP), joka tukee monenkäyttäjän neuvotteluja ja
- Session Description Protocol (SDP), jonka avulla kuvataan multimediayhteyksiä internetissä.

Tämän lisäksi multimediayhteykset käyttävät tietenkin hyväkseen alemman tason protokollia kuten Internet Protocol (IP), Transmission Control Protocol (TCP) ja User Datagram Protocol (UDP). Kuva 1 esittelee näiden protokollien suhteet toisiinsa.

## Session Initiation Protocol (SIP)



Kuva 1. Internetpuheluprotokollien arkkitehtuuri (Fingal & Gustavsson 1999)

Ennen kuin paneudumme syvemmälle SIP-protokollaan, on ehkä syytä esitellä sitä ympäröivät protokollat hieman tarkemmin.

### 4.1 Ympäröivät protokollat

IETF:n multimediaprotokollat ovat itsenäisiä kokonaisuuksia, jotka käyttävät hyväkseen muita protokollia ja joita vuorostaan muut saattavat käyttää hyväkseen.

#### 4.1.1 IP (RFC 791)

IP eli Internet Protocol on nimestäänkin päätellen koko internetin perusta. Se on verkkokerroksen eli OSI-mallin kolmoskerroksen protokolla joka tarjoaa ylemmille kerroksille epäluotettavan yhteydettömän paketsiirtopalvelun. IP siis siirtää datapaketteja verkon läpi ilman että saman alkupisteen ja loppupisteen välisillä paketeilla olisi mitään yhteyttä toisiinsa. Siirrossa käytetään apuna IP-osoitteita, jotka ovat globaaleja 32-bittisiä (tai 128-bittisiä seuraavassa protokollaversiossa, IPv6:ssa) osoitteita.

#### 4.1.2 TCP (RFC 793)

Transmission Control Protocol, TCP, on yhteydellinen neloskerroksen eli siirtokerroksen protokolla. Sillä muodostetaan ja ylläpidetään yhteyttä kahden verkossa olevan ohjelman välillä, jotta ne voivat vaihtaa dataa verkon ylitse. TCP huolehtii datan pilkkomisesta paketteihin, joita

IP-kerros kuljettaa ja vastaavasti toisessa päässä se kokoaa paketit ja muodostaa niistä viestejä tarjottavaksi eteenpäin ylemmille kerroksille.

#### 4.1.3 UDP (RFC 768)

User Datagram Protocol (UDP) on TCP:tä vastaava yhteydetön protokolla. Se tarjoaa yhteydettömän, ilman datagrammien eli tietosähkeiden kuittausta tapahtuvan kuljetuspalvelun verkossa olevien koneiden välille. UDP on tehokas, mutta toisaalta epäluotettava sähkevälitysjärjestelmä koska se ei korjaa siirtovirheitä. Sitä käytetään yleensä kysely- / vastaustoiminnoissa joissa sovellukset itse varmistavat viestien perillemenon ja oikeellisuuden esimerkiksi toistamalla kyselyn mikäli vastausta ei kuulu tietyn ajan kuluessa. UDP on siirtokerroksen (4.) protokolla kuten TCP:kin. SIP voi käyttää joko TCP:n tai UDP:n kuljetuspalvelua, koska siinä on määritelty oma mekanismi luotettavuuden takaamiselle.

#### 4.1.4 RTP (RFC 1889)

Real-time Transport Protocol (RTP) on reaaliaikaisen datan kuten puheen tai videokuvan siirtoprotokolla. Se tarjoaa reaaliaikasovelluksille (kuten esimerkiksi IP-puhelu) palveluita kuten ajastuksen uudelleenjärjestelyä (timing reconstruction), katoamisen seuranta (loss detection), turvallista siirtoa ja sisällön tunnistusta.

#### 4.1.5 RTCP (RFC 1889)

RTP Control Protocol eli RTCP on itse asiassa RTP:n kontrolliosia. RTCP tukee reaaliaikaista neuvottelua minkä tahansa suuruisten ryhmien kesken. Sen tarjoamia palveluita ovat mm. lähteentunnistus ja palvelunlaatupalaute vastaanottajilta lähettäjiille sekä erilaisten datavirtojen synkronointi. Se tukee myös yhdyskäytävien (gateway) kuten audio- ja videosiiltojen (bridges) ja multicast-unicast-konverttereiden (multicast-to-unicast translator) liittämistä verkkoon.

#### 4.1.6 RSVP (RFC 2205)

Resource Reservation Protocol (RSVP) on protokolla joka mahdollistaa internetin kanavien tai polkujen varaamisen laajakaistaisten yhdestä-moneen-lähetysten (multicast) perillemenon turvaamiseksi. RSVP on osa Internet Integrated Service (IIS) –mallia, joka takaa reaaliaikaisen best-effort-palvelun ja linkinjoon valvonnan.

Internetissä normaalisti käytetty ”best-effort” –reititysfilosofia on riittävä niin sanotusti normaaleihin käyttötarkoituksiin kuten teksti- ja kuvamuotoisen datan siirtoon, mutta video- ja audio-ohjelmat vaativat kehittyneempää reititysjärjestelmää yhtäjaksoisten datavirtojen siirtämiseen. RSVP tarjoaa mahdollisuuden varata tietyn kaistan etukäteen ja varmistaa tavallista

luotettavamman datan siirron tietyn käyttäjän tarpeisiin. RSVP tukee niin yhdeltä-yhdelle (unicast), yhdeltä-monelle (multicast) kuin monelta-yhdelle lähetyksiäkin.

#### 4.1.7 RTSP (RFC 2326)

Real-Time Streaming Protocol (RTSP) on sovellustason protokolla joka ohjaa reaaliaikaisen datan siirtoa. Se tarjoaa laajennettavan alustan reaaliaikadatan (esimerkiksi audio tai video) siirtoon ohjatusti ja oikea-aikaisesti (on-demand). Sen tarjoamia palveluita on muun muassa useiden samanaikaisten datansiirtoistuntojen ohjaaminen, mahdollisuus valita siirtokanava kuten UDP, monelta-monelle UDP tai TCP, ja mahdollisuus valita RTP:hen perustuva siirtomekanismi.

#### 4.1.8 SDP (RFC 2327)

Session Description Protocol (SDP) tarjoaa menetelmän multimediatyhteyksien kuvaamiseen ja sitä käytetään hyväksi yhteyksien avaamisessa.

#### 4.1.9 SAP (Internet draft)

Session Announcement Protocol (SAP) tarjoaa palveluita multimediatyhteyksien mainostamiseen multicast-yhteyksien avulla. Sitä käytetään tilanteissa joissa muodostetaan yleisesti kiinnostavia yhteyksiä joiden osanottajia ei tiedetä etukäteen. Jos osanottajat on etukäteen tiedossa, käytetään SIPiä yhteyden muodostamiseen.

## 4.2 SIP-komponentit

SIP määrittelee kolmenlaisia osakokonaisuuksia: käyttäjäagentteja (user agent), välityspalvelimia (proxy server) ja uudelleensuuntauspalvelimia (redirect server).

### 4.2.1 Käyttjäagentti

Käyttjäagentilla on kaksi tehtävää: se kuuntelee tulevia SIP-sanomia ja lähettää niitä joko vastauksina tuleviin viesteihin tai käyttäjän ohjaamana. Tämän lisäksi käyttjäagentti yleensä myös käynnistää tietynlaisia ohjelmia sen perusteella minkälaisen yhteyden se on saanut muodostettua.

Käyttjäagentit käyttävät koodekkeja (codecs) ääni- ja videosignaalien digitoimiseen ja kompressoimiseen. Koodekkeja on monenlaisia - ne eroavat toisistaan mm. äänen tai kuvan

laadun, signaalin siirtoon vaaditun kaistanleveyden ja prosessoritehon käytön suhteen. SIP suosituksen mukaan käyttäjäagentin tulee tukea ainakin G.711, DVI4 ja GSM koodekkeja.

#### 4.2.2 Välityspalvelin

Välityspalvelin välittää SIP-sanomia ja mahdollistaa alueen nimen (domain name) käytön tietyn käyttäjän paikallistamiseen mikäli vastaanottajan IP-osoite tai isäntäkoneen nimi ei ole tiedossa. Välityspalvelinta voi siten käyttää myös käyttäjän olinpaikan piilottamiseen.

Välityspalvelin voi olla joko tilallinen tai tilaton. Tilallinen välityspalvelin muistaa sisääntulevat ja lähtevät pyynnöt ja mitkä sisääntulevista tuottivat mitkään lähtevät. Tilaton palvelin taas unohtaa kaiken pyyntöihin liittyvän tiedon heti kun lähtevä pyyntö on saatu liikkeelle. TCP-yhteyksiä hyväksyvän välityspalvelimen tulee olla tilallinen.

#### 4.2.3 Uudelleensuuntauspalvelin

Uudelleensuuntauspalvelin ei välitä SIP-sanomia vaan palauttaa lähettäjälle vastaanottajan olinpaikan. Nämä palvelimet pystyvät helposti hallitsemaan erittäin suuria käyttäjämääriä, koska ainoa mitä palvelin tekee, on uudelleensuuntaus. Sen ei tarvitse osallistua itse monimutkaiseen välitystapahtumaan.

Sekä välityspalvelin että uudelleensuuntauspalvelin ottaa vastaan käyttäjien rekisteröitymisiä, jossa käyttäjä ilmoittaa senhetkisen olinpaikkansa. Tieto olinpaikasta talletetaan joko näille palvelimille tai erilliselle paikannuspalvelimelle (location server).

### 4.3 SIP-osoitteet

Yhteydenmuodostuksessa täytyy tietää vastaanottavan osapuolen yksiselitteinen osoite. SIPissä osoitteet annetaan käyttäjälle johonkin isäntäkoneeseen, tämä on ns. SIP URL. Sähköpostiosoitteen tyyppinen SIP URL on muotoa käyttäjä@isäntäkone, missä käyttäjä voi olla käyttäjänimi, puhelinnumero tai käyttäjän oikea nimi. Isäntäkone on joko alueen nimi tai numeerinen verkko-osoite. SIP URL voisi olla esimerkiksi

- sip:nasu@cc.hut.fi
- sip:pupu@193.65.169.162

Tämä URL voidaan esimerkiksi sijoittaa verkkosivulle linkiksi niin että sen näpäyttäminen saa aikaan soiton kyseiseen numeroon.

#### 4.4 SIP-sanomat

SIPissä on kahdenlaisia sanomia, pyyntöjä ja vastauksia. Pyyntöjä on kuusi: INVITE, ACK, BYE, OPTIONS, CANCEL ja REGISTER. Vastaukset viestittävät pyynnön onnistumisesta tai epäonnistumisesta, erilaisia vastaus- ja statuskoodeja on useita kymmeniä.

SIP on tekstipohjainen protokolla toisin kuin monet muut signaalointiprotokollat kuten H.323. SIPissä käytetään ISO-10646 ja UTF-8 koodausta. Siksi se on helppo toteuttaa ohjelmointikielillä kuten Java, Perl tai Tcl, sitä on helppo debugata ja ennen kaikkea se on joustava ja helposti laajennettavissa. Tekstipohjaisuudella on myös kääntöpuolensa: otsikoista tulee pitkiä ja niiden jäsentäminen voi olla monimutkaista epäsäännöllisestä rakenteesta johtuen. Koska SIPiä käytetään lähinnä multimedia yhteyksien muodostamiseen eikä niinkään pienten datamäärien hakemiseen, tekstipohjaisuudesta johtuva ylimääräinen kustannus ei liene ongelma. Jäsennettävyyttä on SIPissä pyritty parantamaan määrittelemällä kaikille sanomille ja niiden otsikoille yhteinen rakenne. Pyyntöt ja vastaukset käyttävät geneeristä sanomamuotoa, jonka osia ovat aloitusrivi, yksi tai useampi otsikkokenttä, tyhjä rivi merkitsemään otsikkokenttien päättymistä sekä valintainen viestikenttä. Sanomasyntaksi vastaa HTTP/1.1 spesifikaatiota.

##### 4.4.1 Otsikkokentät

Sanoman otsikossa määritellään muun muassa soittajan osoite, soitettu osoite, sanoman reitti, sanoman tyyppi ja pituus. Osaa otsikkokentistä käytetään kaikissa sanomissa, toisia vain joko pyynnöissä tai vastauksissa. Otsikkokenttien järjestyksellä ei muuten ole merkitystä paitsi että reitti tulee luonnollisesti määritellä oikeassa järjestyksessä ja solmujen väliset (hop-by-hop) otsikot tulee luetella ennen päästä-päähän (end-to-end) otsikoita.

SIP-sovelluksen tulee ohittaa otsikkokentät joita se ei ymmärrä jotta voidaan taata taaksepäin yhteensopivuus eri versioiden välillä.

Otsikkokentät voidaan jakaa yleisiin, sisällöllisiin, pyyntö- ja vastausotsikkokenttiin.

Yleisiä otsikkokenttiä käytetään sekä pyynnöissä että vastauksissa. Näitä ovat

- **Call-ID**, identifioi tietyn yhteyspyynnön tai tietyn käyttäjän rekisteröitymiset .
- **Contact**, sisältää osoitteita joita käytetään eri tarkoituksiin sanomasta riippuen.
- **CSeq** (Command Sequence), identifioi pyynnön Call-ID:n sisällä.
- **Date**, päivämäärä.
- **Encryption**, määrittelee onko sanoman sisältö salattu ja millä algoritmilla.
- **Expires**, viimeinen voimassaolopäivämäärä ja kellonaika.
- **From**, lähettäjän osoite.
- **Record-Route**, voidaan käyttää määrittelemään tulevien pyyntöjen reittiä samalle lähettäjä-vastaanottaja-parille.
- **Timestamp**, asetetaan käyttäjän koneessa, voidaan käyttää mittaamaan pyyntöjen kiertoaikoja.
- **To**, vastaanottajan osoite.
- **Via**, pyynnön tähän mennessä matkaama reitti. Käytetään välttämään silmukoita ja takaamaan se että vastaukset käyttävät samoja reittejä kuin vastaukset.

Sisällölliset otsikkokentät kuvaavat sanoman sisältöä:

- **Content-Length**, sanoman sisällön pituus tavuina.
- **Content-Type**, sisällön tyyppi, esimerkiksi text/html.
- **Content-Encoding**, lisämääritelmä sisällön tyypille.

Pyyntöihin liittyviä kenttiä ovat

- **Accept**, määrittelee mitkä mediatyypit (esimerkiksi application/sdp) hyväksytään vastauksessa.
- **Accept-Encoding**, määrittelee mitkä sisällön koodaustavat sallitaan vastauksessa.
- **Accept-Language**, voidaan käyttää antamaan asiakkaalle mahdollisuus määrittellä millä kielellä se toivoisi että virheilmoitukset, yhteyskuvaukset ja muut sanomien sisällön viestit sille annettaisiin. Voidaan käyttää jopa puhelun vastaanottajan määrittämiseen (esimerkiksi puhelinvaihteessa ohjataan henkilölle joka puhuu toivottua kieltä).
- **Authorization**, käyttäjäagentti voi käyttää henkilöllisyytensä todistamiseen serverille esimerkiksi "410 Unauthorized" virheilmoituksen jälkeen. Kenttä sisältää käyttäjäagentin autentikointitiedot pyydetylle resurssille.
- **Hide**, käytetään osoittamaan että asiakas haluaa piilottaa Via-otsikkokentässä näkyvän polun seuraavilta välityspalvelimilta ja käyttäjäagenteilta.
- **Max-Forwards**, voidaan käyttää rajoittamaan niiden välityspalvelinten ja yhdyskäytävien määrää, jotka saavat välittää pyyntöä eteenpäin. Hyödyllinen epäonnistuvien pyyntöjen jäljittämisessä.
- **Organization**, pyynnön lähettäjän organisaatio tai yhteisö.
- **Priority**, asiakkaan määrittelemä pyynnön kiireellisyys (häätätapaus, kiireellinen, normaali, ei kiireellinen).
- **Proxy-Authorization**, sama kuin Authorization, mutta välittää autentikointitiedon vain seuraavalle välityspalvelimelle joka pyysi asiakkaalta henkilöllisyyden todistamista (Proxy-Authenticate -kentällä).
- **Proxy-Require**, välityspalvelimelta vaaditut ominaisuudet.
- **Require**, asiakkaan määrittelemät käyttäjäagentin palvelimelta vaaditut ominaisuudet.
- **Response-Key**, asiakas voi tällä kentällä pyytää vastaanottavalta käyttäjäagentilta avainta jolla tämä salaa vastauksen.

## Session Initiation Protocol (SIP)

- **Route**, määrittelee pyynnön kulkeman reitin.
- **Subject**, puhelun aihe (voidaan käyttää mm. puhelujen suodatuksessa).
- **User-Agent**, sisältää tietoja pyynnön lähettävän asiakkaan käyttäjäagentista.

Vastauksiin liittyvät kentät:

- **Allow**, lista lähettäjän tukemista metodeista.
- **Proxy-Authenticate**, henkilöllisyyden todistamispyyntö, sisältää kuvauksen vaaditusta autentikointitavasta ja -parametreista.
- **Retry-After**, vastaanottaja voi tällä kentällä viestittää soittajalle arvion siitä kuinka kauan se tulee olemaan tavoittamattomissa, käytetään siis joidenkin virheilmoitusten yhteydessä.
- **Server**, sisältää tietoja pyynnön lähettävän asiakkaan käyttäjäagenttipalvelimesta.
- **Unsupported**, lista piirteistä joita palvelin ei tue.
- **Warning**, käytetään antamaan lisäinformaatiota vastauksen tilasta.
- **WWW-Authenticate**, henkilöllisyyden todistamispyyntö, sisältää kuvauksen vaaditusta autentikointitavasta ja -parametreista.

### 4.4.2 Pyynnöt

Pyynnöissä aloitusrivinä on ns. pyyntöriivi (Request-Line), joka sisältää metodin nimen, vastaanottajan osoitteen ja protokollan versionumeron. Metodeja eli erilaisia pyyntöjä on siis nykyisessä SIP-versiossa kuusi. Seuraavassa taulukossa on lueteltu niiden toiminta:

INVITE	INVITE-metodilla käyttäjä tai palvelu kutsutaan osallistumaan istuntoon. Kahdenvälisessä puhelussa soittaja määrittelee mitä mediatyyppejä se pystyy vastaanottamaan sekä niiden parametrit kuten verkko-osoitteet.
ACK	ACK-pyyntö vahvistaa asiakkaan saaneen lopullisen vastauksen INVITE-pyyntöönsä. Sen viestikentässä voidaan välittää lopullinen istunnonkuvaus jota vastaanottajan tulee käyttää.
BYE	Käyttäjäagenttiasiakas käyttää BYE-viestiä osoittamaan palvelimelle haluavansa lopettaa puhelun.
CANCEL	CANCEL-viestillä voi perua pyynnön jota ei vielä ole viety loppuun. Viesti katsotaan loppuun viedyksi kun palvelin on lähettänyt viimeisen osan vastauksesta.
OPTIONS	OPTIONS-metodia käytetään välittämään tietoa osapuolten ominaisuuksista ja kyvyistä.
REGISTER	REGISTER-viestillä välitetään SIP-palvelimelle tietoa käyttäjän olinpaikasta.

## Session Initiation Protocol (SIP)

Pyyntöriivin jälkeen luetellaan tarvittavat otsikkokentät sisältöineen. Viestiin voidaan lisätä käytetyn istunnon kuvaus. Se erotetaan otsikkokentistä tyhjällä rivillä ja sen käyttämä mediatyyppi tulee määritellä Content-Type-otsikkokentässä.

Esimerkki SIP-pyyntöstä:

```
INVITE sip:pup@kolo.fi SIP/2.0
Via: SIP/2.0/UDP possu.laava.fi
From: Nasu <sip:nasu@laava.fi>
To: Pupu <pup@kolo.fi>
Call-ID: 1234567890@laava.fi
CSeq:1 INVITE
Subject: Mitä kuuluu?
Content-Type: application/sdp
Content-Length: 5678
```

```
v=0
o=ffl 53274623 6853680975 IN IP4 123.5.4.3
s=kysely
c=IN IP4 possu.laava.fi
m=audio 5004 RTP/AVP 0 3 5
```

Tässä siis nasu@laava.fi lähetti INVITE-pyyntön osoitteeseen pup@kolo.fi jossa on SDP:n (Session Description Protocol) mukainen istuntokuvaus. Siinä v-parametrissa on protokollan versio, o:ssa istunnon omistaja ja tunnistin, s:ssä istunnon nimi, c:ssä tietoja yhteydestä ja m:ssä median nimi ja lähetysosoite. Tässä tapauksessa nasu@laava.fi haluaa RTP-audiota porttiin 5004 jossain seuraavista formaateista: PCMU (0), GSM (3) tai DV14 (5).

### 4.4.3 Vastaukset

Vastausviesteillä palautetaan lähettäjälle tieto pyynnön onnistumisesta tai epäonnistumisesta ja sen syystä. Vastauksen tyyppi ilmoitetaan statuskoodilla joka on kolminumeroinen luku. Luvun ensimmäinen numero ilmoittaa vastauksen luokan:

1xx	Tiedonanto
2xx	Onnistuminen
3xx	Uudelleensuuntaus
4xx	Virhe pyynnössä
5xx	Virhe palvelimessa
6xx	Yleinen virhe (koko verkossa)

Ensimmäisen luokan koodeja käytetään edistymisen indikoimiseen, muita käytetään SIP-pyyntön päättämiseen.

SIP sovellusten ei ole välttämätöntä tunnistaa kaikkia rekisteröityjä vastauskoodeja. Vastauskoodin luokka tulee kuitenkin tunnistaa ja kaikki tuntemattomat koodit tulee käsitellä kuten vastausluokan pääkoodi, x00.

Tässä muutama yleisimmin käytetyistä vastauskoodeista:

180	RINGING
200	OK
302	MOVED TEMPORARILY
404	NOT FOUND
501	NOT IMPLEMENTED
600	BUSY EVERYWHERE

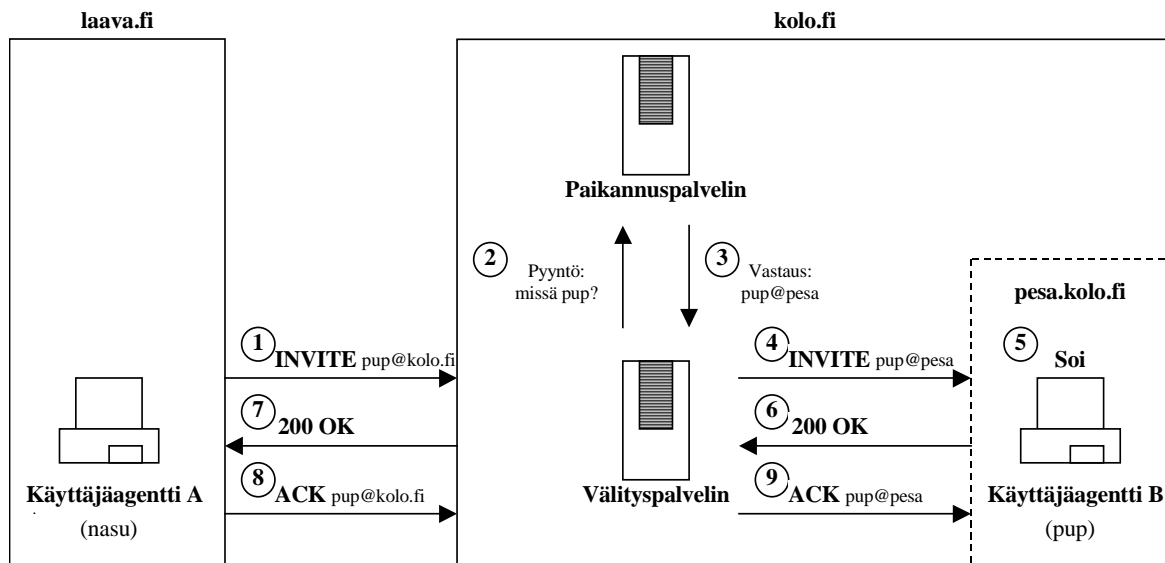
## 4.5 Esimerkki SIP-sanomien kulusta

### 4.5.1 Välityspalvelimen käyttö

Kuva 1 esittää miten välityspalvelimen käyttö tapahtuu yksinkertaisen INVITE-metodin käyttöesimerkin avulla. Tässä ei siis ole kuvattu kaikkien SIP-sanomien välitystä.

Käyttäjäagentti A eli nasu@laava.fi lähettää ensin INVITE-pyynnön osoitteelle pup@kolo.fi (1). Välityspalvelin hyväksyy pyynnön ja pyytää edelleen paikannuspalvelimelta vastaanottajan tarkempaa osoitetta (2). Saatuaan tarkan osoitteen (3) välityspalvelin välittää INVITE-pyynnön edelleen vastaanottajalle tähän osoitteeseen (pup@pesa.kolo.fi) (4). Vastaanottaja saa tiedon kutsusta (5) ja hyväksyy sen lähettämällä vastauksen 200 OK (6). Välityspalvelin välittää tämän viestin Nasulle (7) ja tämä lähettää takaisin kuittauksen (8) jonka välityspalvelin taas välittää oikeaan osoitteeseen (9).

## Session Initiation Protocol (SIP)



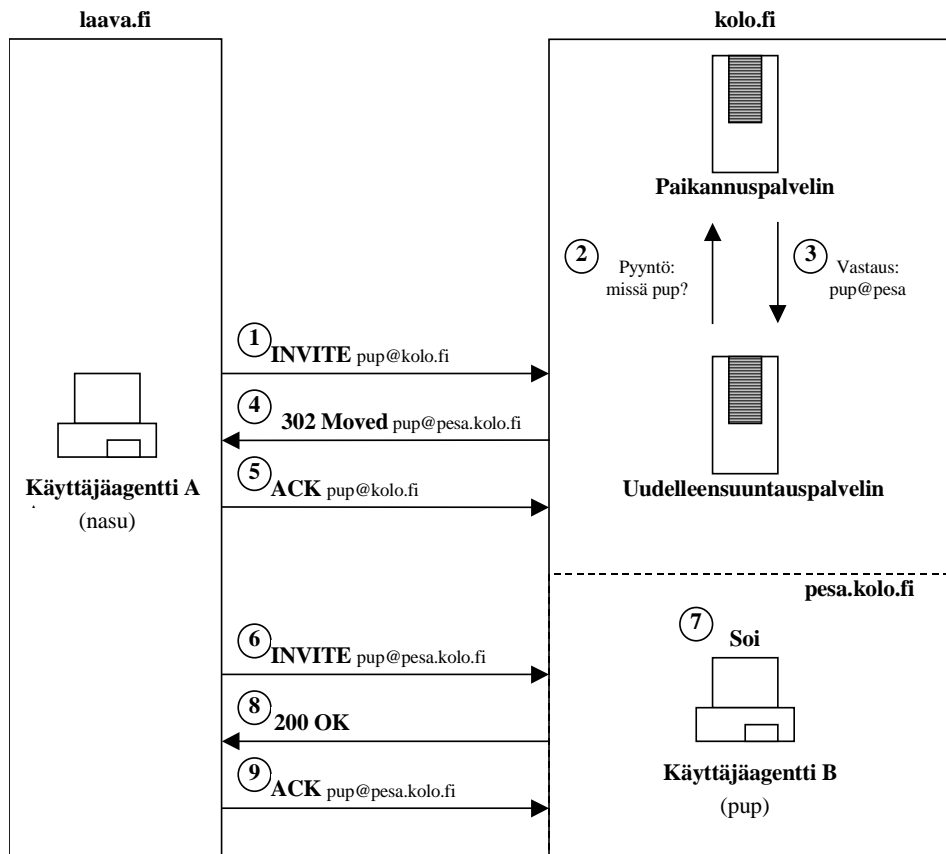
Kuva 2 Esimerkki välityspalvelimen käytöstä

### 4.5.2 Uudelleensuuntauspalvelimen käyttö

Uudelleensuuntauspalvelin ei siis osallistu itse välitystapahtumaan, se ainoastaan välittää lähettäjälle tiedon vastaanottajan nykyisestä olinpaikasta.

Kuva 3 esittelee esimerkin uudelleensuuntauspalvelimen käytöstä. Siinä jälleen nasu@laava.fi lähettää INVITE-kutsun osoitteeseen pup@kolo.fi (1). Nyt uudelleensuuntauspalvelin vastaanottaa viestin, tiedustelee paikannuspalvelimelta Pupun tarkan olinpaikan (2,3) ja lähettää Nasulle vastauksena tiedon siitä että vastaanottaja on toisessa osoitteessa (302 MOVED TEMPORARILY) sekä uuden osoitteen (4). Nasu kuittaa saamansa tiedon (5) ja pystyy nyt lähettämään INVITE-pyyntönsä suoraan oikeaan osoitteeseen (eli pup@pesa.kolo.fi) (6), saa sieltä hyväksyvän vastauksen 200 OK (8) ja kuittaa lopuksi tämän (9).

## Session Initiation Protocol (SIP)



Kuva 3 Esimerkki uudelleensuuntauspalvelimen käytöstä

### 4.6 Turvallisuusnäkökohdat SIP:ssä

Koska SIP-sanomat saattavat sisältää arkaluontoista tietoa puhelun sisällöstä ja osapuolten kommunikointitavoista, sanomien salaaminen on tärkeä osa protokollaa. SIP tukee kolmea erilaista salaamistapaa:

- Päästä-päähän salaaminen (end-to-end encryption) SIP sanoman sisällölle ja muutamalle arkaluontoiselle otsikkokentälle.
- Väli-väliltä salaaminen (hop-by-hop encryption) suojaamaan yhteyttä sen salakuuntelulta kuka on kenellekin soittanut.
- Väli-väliltä salaaminen Via-otsikkokentille jotta pystytään piilottamaan sanoman käyttämä reitti.

Päästä-päähän salausta ei voi käyttää koko SIP-sanomalle koska kaikkien välittäjäpalvelimien tulee nähdä tietyt otsikkokentät (To, Via) jotta ne pystyvät reitittämään sanoman. Väli-väliltä salauksessa voidaan koko sanoma salata ja näin estää linjan salakuuntelu. Päästä-päähän salatut sanomat voidaan myös salata väli-väliltä.

Nämä salausmetodit suojaavat siis SIP-sanomaa, mutta henkilö joka todella haluaa tietää minkälaista liikennettä verkossa kulkee, voi löytää muita keinoja: välityspalvelimet tietävät kuka on soittanut kenellekin ja tämän informaation voi myös saada selville analysoimalla koko verkon liikennettä. Joten SIPin tarjoama suoja on siis rajallista - mutta sen käyttäminen on silti suositeltavaa.

Via-otsikkokenttää käytetään reitittämään vastaus takaisin samaa reittiä kuin sitä vastaava pyyntö ja estämään loputtomien vastaussilmukoiden syntymistä. Sen sisältämä tieto voi kuitenkin olla hyödyllistä myös salakuuntelijalle tai vihamieliselle hyökkääjälle. Hide-otsikkokentän avulla käyttäjä voi salata Via-kentän sisältämän reitin välittäjäpalvelimilta ja käyttäjäagenteilta.

Päästä-päähän salaus perustuu osapuolten käyttäjäagenttien vaihtamiin salausavaimiin. Tyypillisesti sanoma lähetetään vastaanottajan julkisella avaimella salattuna niin että vain vastaanottaja pystyy purkamaan viestin. Kaikkien SIP-palvelinten tulee tukea PGP-salausmenetelmää (Pretty Good Privacy), muut menetelmät ovat valinnaisia.

Väli-väliltä salaus tapahtuu joko verkko- tai kuljetuskerroksella. SIP suosituksessa ei määritellä mitään tiettyä salausmekanismia väli-väliltä salaukseen, mutta mainitsee vaihtoehtoina IPSEC:n (Internet Protocol Security Architecture) ja TLS:n (Transport Layer Security). Salausmekanismin valinta tehdään yleensä käsin konfiguroimalla, ei dynaamisesti.

## 5 SIPin tarjoamat palvelut

IP-puhelujärjestelmien arkkitehtuurissa on suuria eroja perinteiseen puhelinverkkoon verrattuna. Niissä lähdetään siitä että kaikki signaalintieto ja data liikkuu IP-pohjaisessa verkossa, joko intranetissä tai julkisessa Internetissä. Tämä tuo suuren muutoksen verkon solmujen väliseen yhteydenpitoon verrattuna perinteiseen puhelinverkkoon joissa solmut pystyvät (hieman yksinkertaistetusti) keskustelemaan vain suoraan niihin yhteydessä olevien solmujen kanssa. IP-

verkossa jokainen verkon kone voi keskustella minkä tahansa toisen verkossa olevan koneen kanssa mikäli tätä ei ole nimenomaisesti estetty esimerkiksi palomuurilla.

Tämä eroavaisuus perinteisten puhelinverkkojen ja IP-verkkojen välillä on aiheuttanut sen että myös palvelujen arkkitehtuuri on hyvin erilainen näissä verkoissa. Yleisesti ottaen päätejärjestelmien oletetaan internetarkkitehtuurissa olevan huomattavasti älykkäämpiä kuin perinteisissä puhelinverkoissa. Tästä johtuen monia ennen verkon suorittamia palveluja on IP-verkoissa voitu siirtää verkon reunoille päätejärjestelmiin.

Pystyäkseen kilpailemaan perinteisten puhelinverkkojen kanssa, SIP-puhelujen tulisi luonnollisesti pystyä tarjoamaan vähintään samat palvelut. Lennox, Schulzrinne ja La Porta ovat selvittäneet kuinka ITU-T:n määrittämät älyverkkopalvelut voidaan toteuttaa SIPillä (Lennox *et al.* 1999). Suurin osa ITU-T Q.1211 standardin määrittelemistä palveluista voidaan toteuttaa SIP-järjestelmässä joko itse verkossa tai sen päätejärjestelmissä, osa näistä vaatii SIPin puhelunohjaus laajennuksen käyttöä (Schulzrinne & Rosenberg 1998).

Laskutuksen järjestäminen on kuitenkin ongelmallista IP-verkoissa ja joitain siihen liittyviä palveluita ei vielä pystytä SIP-puheluilla tarjoamaan. IP-puhelujen suhteen on itseasiassa vielä avoinna se mitä palveluja voidaan ylipäätään laskuttaa. Palveluista jotka toteutetaan päätejärjestelmissä ei tietenkään voi laskuttaa käytön mukaan, näistä on mahdollista saada vain päätelaitteen ohjelmiston myynnin kertamaksu. Laskutuksen ongelman käsittely ei kuitenkaan sinänsä liity signaalintikysymyksiin, niitä laskutustiedon välityksen standardoittotyö on meneillään IETF:n Internet Open Trading Protocol työryhmässä.

Tässä muutama esimerkki palveluista joiden tarjoamiseen SIP tarjoaa protokollamekanismit:

- Puhelun edelleenvälitys (call forwarding), sisältäen seuraavat palvelut:
  - Edelleenvälitys kun ei vastausta
  - Edelleenvälitys kun varattu
  - Edelleenvälitys ilman ehtoja
  - Muut osoitteenmuunnospalvelut
- Soittajan ja vastaanottajan ”numeron” välitys (numero voi olla minkä tahansa mieluiten yksikäsitteisen nimeämiskäytännön mukainen tunniste)
- Henkilökohtainen numero: toiminto jossa vastaanottaja on tavoitettavissa samasta olinpaikasta riippumattomasta osoitteesta vaikka hänen käyttämänsä päätelaite vaihtuisi

## Session Initiation Protocol (SIP)

- Päätelaitetyypin neuvottelu ja valinta: toiminto jossa soittaja voi määrittellä miten vastaanottajaa tulisi tavoitella (esim. IP-puhelin, matkapuhelin, vastaajapalvelu, jne.)
- Päätelaitteen ominaisuuksien neuvottelu
- Soittajan ja vastaanottajan tunnistaminen
- Näkymätön ja ohjattu puhelun siirto
- Yhdeltä-monelle puhelinneuvottelukutsu

### 5.1 Käyttäjän liikkuvuus

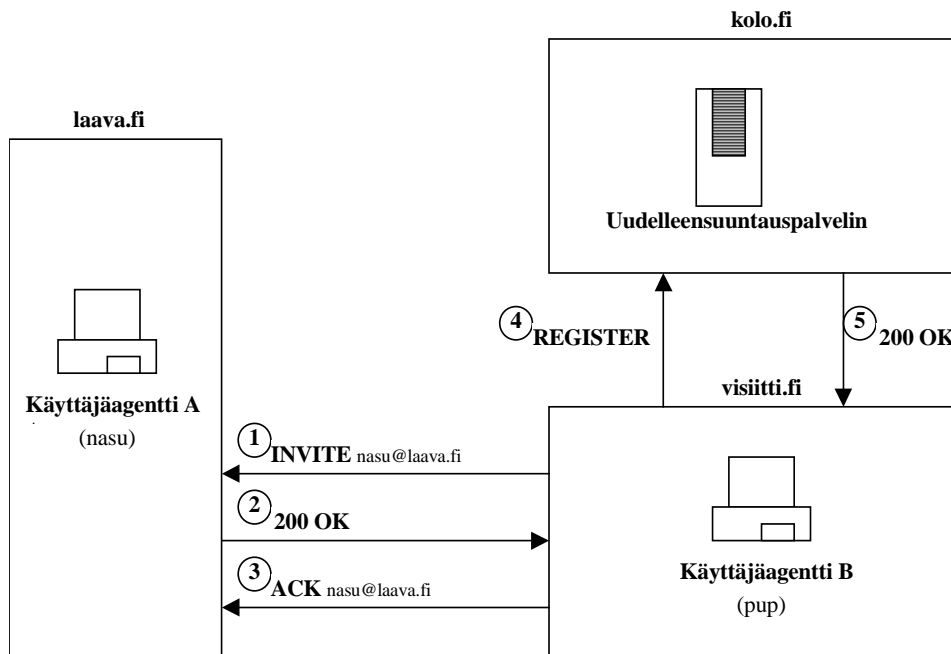
SIP siis tukee henkilökohtaisen puhelinnumeron käsitettä, eli vastaanottaja pystytään löytämään hänen olinpaikastaan tai käyttämästään päätelaitteesta (esim. PC, IP-puhelin) riippumatta. SIP-palvelimet tekevät tämän mahdolliseksi, koska käyttäjä voi rekisteröityä mille tahansa palvelimelle olinpaikasta riippumatta ja hänet löydetään vaikka hän vaihtaisi olinpaikkaa tai päätelaitetta. Tätä piirrettä voidaan kutsua liikkuvuudeksi ennen puhelua (pre-call mobility).

Liikkuvuus kesken puhelun (mid-call mobility) tarkoittaa käyttäjälle läpinäkyvää siirtymistä yhden IP-aliverkon alueelta toiselle. Tukeakseen ennen puhelua tapahtuvan liikkuvuuden lisäksi liikkuvuutta kesken puhelun, SIP-protokollan tulisi kyetä tarjoamaan keino käyttäjän IP-osoitteen vaihtumiseen kesken istunnon.

Tässä kuvaus siitä miten SIP tukee käyttäjän liikkumista aliverkon alueelta toiselle kesken puhelun (Wedlund & Schulzrinne 1999):

Oletetaan että liikkuvalla päätelaitteella (esim. matkapuhelin tai kannettava PC) on ns. kotiverkko, jonka SIP-palvelimelle (tässä tapauksessa oletetaan se uudelleensuuntauspalvelimeksi) se rekisteröityy joka kerta vaihtaessaan olinpaikkaa. Kun joku lähettää INVITE-pyynnön liikkuvalla isäntäkoneelle, uudelleensuuntauspalvelin pystyy ohjaamaan sen oikeaan osoitteeseen, koska rekisteröityessään liikkuva isäntäkone on kertonut senhetkisen olinpaikkansa.

## Session Initiation Protocol (SIP)



**Kuva 4** Esimerkki liikkuvan isäntäkoneen toiminnasta

Jos isäntäkone liikkuu kesken istunnon, sen täytyy lähettää uusi INVITE-pyyntö sitä kutsuneelle vastapuolelle käyttäen samaa puhelutunnistetta kuin alkuperäisessä puhelun aloituksessa. Sen tulee laittaa uusi IP-osoitteensa SIP-sanoman Contact-kenttään, joka kertoo vastapuolelle mihin se haluaa vastaanottaa tulevat sanomansa. Uusi osoite laitetaan myös sanoman istunnonkuvausosan (SDP) c-kenttään. From-kenttään tulee kuitenkin laittaa kotiverkon osoite, koska sitä käytetään tunnistuksessa ja sitä voi myös käyttää varakeinona mikäli yhteys sattuisi katkeamaan. Lopuksi liikkuvan isäntäkoneen tulee rekisteröityä kotiverkkonsa SIP-palvelimelle ja kertoa senhetkinen osoitteensa jotta uudet puhelut voidaan ohjata oikeaan paikkaan.

Kuva 4 on esitetty esimerkki liikkuvasta vastaanottajasta. Siinä Kuva 3:n mukaisesti luotu yhteys jatkuu vaikka vastaanottaja (kotiosoitteeltaan pup@kolo.fi) siirtyy toisen verkon (visiitti.fi) alueelle kesken puhelun.

Tulee huomata että edellä kuvattu liikkuvuuden tuki toimii vain käytettäessä UDP-yhteyksiä; TCP-yhteydet vaatisivat käyttäjälle näkymätöntä IP-osoitteen vaihtumista. Tällaisen läpinäkyvän liikkuvuuden tarjoava menetelmä on esitelty RFC 2002:ssa (Perkins 1996), kutsuttakoon sitä tässä IP-liikkuvuudeksi. IP-liikkuvuudessa on kuitenkin useita haittapuolia: ensinnäkin siinä käytetään ns. kolmioreititystä (triangular routing), missä soittajalta puhelun vastaanottajalle menevä paketti kuljetetaan kotiverkon kautta ja toiseen suuntaan menevä paketti suoraan

soittajalle. Toiseksi liikkuva isäntäkone tarvitsee pysyvän osoitteen kotiverkkoonsa, mikä saattaa aiheuttaa ongelmia nykyisen IP-verkon osoiteavaruuden rajallisuuden vuoksi. Toisaalta tietyissä TCP:tä käyttävissä palveluissa kuten webin selailu tai sähköpostin haku käyttäen SMTP:tä (Simple Mail Transfer Protocol), POP:ia (Post Office Protocol) tai IMAP:ia (Internet Message Access Protocol) TCP-yhteydet ovat yleensä niin lyhyitä, että uudelleenlähettykset ovat hyväksyttävissä. Tästä syystä on ehdotettu että IP-liikkuvuutta käytettäisiin pitkäkestoisille TCP-yhteyksille kuten telnet, ftp ja irc, kun taas edellä esitettyä SIPin kautta toteutettua liikkuvuutta tosiaikaisille yhteyksille UDP:n päällä (Wedlund & Schulzrinne 1999). Tällainen liikenteen jakaminen liikkuvuuskäsittelyn mukaan vaatisi kuitenkin ns. liikkuvuuskäsittelytaulun (mobile policy table) lisäystä protokollapinoon.

## 6 Muut VoIP-standardit

### 6.1 H.323

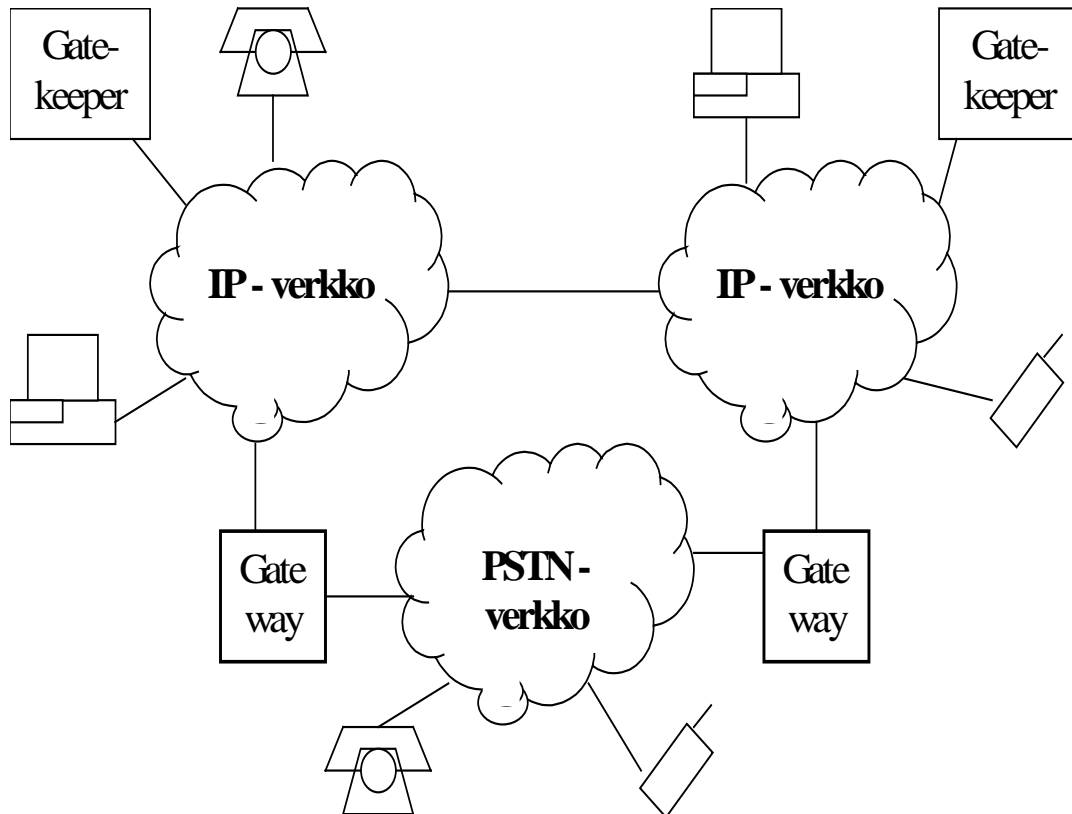
ITU-T:n suositus H.323 kuvaa tekniset vaatimukset multimediatelekomunikaatiopalveluille pakettikytkentäisessä verkossa. Se on itseasiassa kattosuositus useammalle ITU-T-standardille. Suositus ei puutu verkkorajapintaan, verkon fyysiseen rakenteeseen tai verkon siirtoprotokollaan.

H.323:ssa on määritelty neljä pääkomponenttia: terminaali, gateway eli yhdyskäytävä, gatekeeper ja ns. konferenssikontrolliyksikkö (Multipoint Control Unit, MCU). Terminaalit, gatewayt ja MCU:t luokitellaan verkkopäätepisteiksi (endpoints) eli laitteiksi jotka voivat lähettää ja vastaanottaa puhelua.

H.323-terminaalit ovat asiakaspäätepisteitä jotka tarjoavat reaaliaikaista kahdensuuntaista kommunikaatiota. Ne vastaavat suunnilleen SIPin käyttäjäagentteja. Kaikkien terminaalien tulee tarjota reaaliaikaisen äänen välitystä, videokuvan ja datan välityksen tuki on laitevalmistajalle vapaaehtoista. Terminaalit voidaan toteuttaa joko PC-ohjelmistoina tai erillisinä laitteina kuten kuvapuhelimina tai internetpuhelimina.

H.323-gateway puolestaan on verkkopäätepiste joka tarjoaa reaaliaikaista, kahdensuuntaista kommunikaatiota joko H.323-terminaalien ja muiden ITU:n määrittelemien päätelaitteiden (esimerkiksi puhelinten) tai kahden gatewayn välillä. Ne huolehtivat puhelunohjauksen ja puhelun sisällön muuntamisesta pakettiverkosta piirikytkentäiseen verkkoon ja toisin päin.

Gatewayta tarvitaan H.323-verkossa vain mikäli siitä halutaan yhteyksiä muihin verkkoihin kuten perinteiseen puhelinverkkoon, se ei siis ole välttämätön laite H.323-verkossa.



**Kuva 5** Kaavakuva H.323-verkosta

Konferenssikontrolliyksikkö (Multipoint Control Unit, MCU) tarjoaa palveluita jotka mahdollistavat kolmen tai useamman verkkopäätteen osallistumisen ns. konferenssipuheluun (conference call). MCU:ssa on kontrolleri (Multipoint Controller, MC), joka tarjoaa konferenssipuheluun tarvittavat puhelunohjaustoiminnot, ja mahdollisesti myös prosessori (Multipoint Processors, MP), joka prosessoi (sekoittaa tai kytkee) ääni-, videokuva- ja/tai datavuot. MCU-toiminnot on voitu toteuttaa myös jossain muussa H.323-laitteessa: terminaalissa, gatewayssa tai gatekeeperissä.

H.323-suosituksen mukaan kaikkien verkkopäätteen tulee tukea G.711-standardin mukaista äänikoodekkia. Näin varmistetaan että aina löytyy ainakin yksi yhteinen kieli. Mikäli laite tukee

myös videokuvan välitystä, tulee sen tukea ainakin H.261 suosituksen videokoodekkia. Puhelun aloituksen yhteydessä osapuolet neuvottelevat siitä mitä koodekkia kukin verkkopäätepiste käyttää.

Gatekeeper on valinnainen H.323-komponentti, joka tarjoaa monia tärkeitä palveluja kuten aluevalvonta (zone control), kulunvalvonta (admission control), kaistanleveyden valvonta (bandwidth control) ja osoitteenmuunnos (address translation). Alue- ja kulunvalvonta liittyvät gatekeeper-alueen käsitteeseen: se on kaikkien niiden terminaalien, yhdyskäytävien ja MCU:iden joukko jotka ovat yhden gatekeeperin hallinnassa. Kulunvalvonta tarkoittaa sitä että gatekeeper antaa tai kieltää oikeuden käyttää hallitsemaansa aluetta esimerkiksi vapaan kaistanleveyden perusteella. Gatekeeper pitää yllä tietokantaa kaikista sen hallinnassa olevista verkkopääteistä. Se huolehtii myös selväkielisten pääteistenimien (esim. isäntäkoneen nimi tai sähköpostiosoite) ja ulkoisten osoitteiden (esimerkiksi E.164-puhelinnumeroiden) muuntamisesta verkko-osoitteiksi (esimerkiksi IP-osoitteiksi). Muita gatekeeperin mahdollisesti tarjoamia palveluita ovat puheluoikeuksien tarkistaminen (call authorization), kaistanleveyden hallinta (bandwidth management), puhelujenhallinta (call management) ja puhelunohjauksen signalointi (call control signalling).

## 6.2 SIP:n ja H.323:n vertailu

Tässä kappaleessa vertaillaan näitä kahta VoIP-protokollaa erilaisten ominaisuuksien suhteen, lähinnä on keskitytty ominaisuuksiin jotka eroavat paremmuudeltaan toisistaan eri protokollissa.

Yleisesti voidaan sanoa että protokollat lähentyvät jatkuvasti toisiaan toiminnallisuutensa suhteen. H.323:n versio 3 tarjoaa jo hyvin pitkälle samat toiminnot kuin SIP, aiemmat versiot ovat olleet toiminnaltaan selkeästi suppeampia.

### 6.2.1 Toiminnan yksinkertaisuus

H.323 on verrattain monimutkainen protokolla. Se sisältää useita eri aliprotokollia ja monet palvelut vaativat näiden aliprotokollien vuorovaikutusta keskenään.

SIP ja SDP sen sijaan ovat toiminnaltaan yksinkertaisempia. Yksinkertaisin SIP IP-puhelutoteutus vaatii vain neljän otsikkokentän (To, From, Call-ID ja Cseq) ja kolmen

pyyntösanoman (INVITE, ACK ja BYE) implementoimista. Yksinkertainen toiminta tarkoittaa myös parempaa skaalautuvuutta suuriinkin verkkoihin ja käyttäjämääriin.

### 6.2.2 Kyvykkyystietojen vaihto (capability exchange)

Lähettäjä ja vastaanottaja vaihtavat tietoja toistensa kyvykkyudesta puhelun alustuksessa jotta lähettäjä osaa lähettää vain sen muotoista dataa mitä toinen osapuoli kykenee vastaanottamaan.

H.323 käyttää H.245-protokollaa kyvykkyystietojen vaihtoon. Siinä osapuolet vaihtavat kaiken tiedon toistensa kyvykkyudesta erittäin yksityiskohtaisella tasolla ja suhteellisen kompaktisti.

SIPissä käytetään SDP:tä ja OPTIONS- metodia kyvykkyysinformaation vaihtoon. SDP ei ole yhtä ilmaisukykyinen kuin H.245, se ei esimerkiksi tue asymmetristen kykyjen eli vain lähetyksessä tai vastaanotossa käytettyjen kykyjen vaihtoa.

### 6.2.3 Toiminnallisuuden laajennettavuus

Koska IP-puhelutekniikat ovat hyvin nuoria, on erittäin todennäköistä että uutta signaalintoittoiminnallisuutta joudutaan lisäämään niihin vielä melko paljon.

H.323:ssa on yksi laitevalmistajakohtainen kenttä (NonStandardParam), jota voi käyttää uusien toiminnallisuuksien implementointiin.

SIP tarjoaa joustavammat mahdollisuudet toiminnallisuuden laajentamiseen. Siinä käytetään hierarkista piirteiden nimeämismekanismia ja hierarkisesti järjestettyjä numeerisia virhekoodeja.

### 6.2.4 Yhteensopivuus muiden signaalintiprotokollien kanssa

H.323 suositusperheessä on useita standardeja joiden tarkoitus on nimenomaan tarjota yhteensopivuus piirikytkentäisten verkkojen kanssa, esimerkiksi H.320 ISDN:lle ja B-ISDN:lle.

SIPissä ei toistaiseksi vielä ole yksityiskohtaista menetelmää muiden signaalintiprotokollien muuntamiseksi SIP-muotoon. Aiheesta on kylläkin kirjoitettu Internet Draft ”A Functional Description of SIP-PSTN Gateway”.

### 6.2.5 Toteutuksen yksinkertaisuus

H.323 signalointisanomat on binäärikoodattu käyttäen ASN.1 (Abstract Syntax Notation One) PER (Packet Encoding Rules) menetelmää. Tämä vaatii informaation muuntamista useaan otteeseen, toisaalla ihmisille ymmärrettävään muotoon ja toisaalla varastoitavaan ja siirrettävään muotoon. Nämä muunnokset vaativat tietynlaisen jäsentäjän käyttöä, mikä tekee toteutuksesta ja virheiden paikannuksesta monimutkaista.

SIP sanomat ovat tekstipohjaisia ja niissä käytetään ISO 10646 ja UTF-8 koodausta. Tekstipohjaisuus helpottaa toteutusta, joka voidaan tehdä esimerkiksi Java, Tcl tai Perl -kielillä, sekä myös virheiden paikannusta.

### 6.2.6 Vikasietoisuus

H.323 versio 3 tukee kahdennettuja gatekeepereitä ja verkkopäätepisteitä ja on siten vikasietoisempi kuin SIP. Siinä gatekeeper voi rekisteröityessään määritellä vaihtoehtoisia gatekeepereitä joita verkkopäätepiestet voivat käyttää ensisijaisen laitteen vioittuessa. Samaten verkkopäätelaitteet voivat määritellä itselleen varaosoitteen.

### 6.2.7 Kolmannen osapuolen ohjaus

Tämä piirre on toistaiseksi määritelty vain SIPissä. Kolmannen osapuolen ohjauksella (Third-Party Control) tarkoitetaan kolmannen osapuolen kykyä muodostaa puhelu kahden muun osapuolen välille osallistumatta siihen itse. SIPin joustavien otsikoiden ansiosta tämän piirteen toteutus on siinä helppoa.

## 7 SIP tuotteet markkinoilla

SIP tuotteita löytyy markkinoilta toistaiseksi vain vähän. Muutama H.323-gatewayvalmistaja on rakentanut tuotteeseensa myös SIP-tuen, mm. Ericsson ja Lucent. Nortel, 3Com ja Ellementel ylläpitävät julkisia SIP-palvelimia, joille voi rekisteröityä ja joiden kautta voi reitittää puhelua.

Yksi SIP-edelläkävijöitä on amerikkalaisyritys nimeltä dynamicsoft, joka julkisti tammikuussa 1999 ensimmäisen pelkästään SIP-protokollaa tukevan välityspalvelimen. Heidän eConvergence Server Solutions -tuotepiheensä käsittää nyt jo välityspalvelimen ja käyttäjäagentin lisäksi

muitakin IP-puhelutuotteita kuten mm. SIP paikannuspalvelimen ja puhelunmonitorointipalvelimen.

Suurin osa SIP-käyttäjäägenttitoteutuksista on vielä yritysten ja yliopistojen tutkimuspöydillä. Agenteja on tehty mm. Kalifornian, Lontoon, Luulajan ja Columbian yliopistoissa. Myös Lucent on tehnyt SIPiä tukevan käyttäjäagentin (Siphone). Pingtel-niminen nuori amerikkalaisyritys on luvannut julkistavansa SIPiä tukevan IP-puhelimensa vuoden 1999 lopussa ja aloittavansa tuotteidensa toimitukset vuoden 2000 alussa.

Tuotteiden valmistajat ja tutkijat ovat pitäneet yhteisiä yhteensopivuustestitilaisuuksia, joissa he testaavat omien laitteidensa toimintaa muiden valmistajien laitteiden kanssa. Erääseen tällaiseen tilaisuuteen otti elokuussa 1999 osaa yhteensä 13 yritystä tai yliopistoa: 3Com, 8x8, Bell Labs, BroadSoft, Cisco Systems, Columbia University, dynamicsoft, Ericsson Inc, MCI WorldCom, Mitel Corp., Nortel Networks, Pingtel Corp ja University of Waterloo.

## 8 Tulevaisuus

IP-pohjaisessa puhelinliikenteessä on monta etua perinteiseen puhelinverkkoon verrattuna: tekniikka on huomattavasti yksinkertaisempaa koska älykkyys on siirretty itse verkosta sen reunoille ja siinä pystytään käyttämään verkon kapasiteetti paljon tehokkaammin hyväksi. Tästä johtuen IP-puhelutekniikka on huomattavasti edullisempaa kuin perinteinen puhelinverkkotekniikka.

IP-puheluiden tulevaisuus siis näyttää valoisalta. Vaikkakin tällä hetkellä niiden osuus kaikesta maailman puhelinliikenteestä on alle prosentin luokkaa, osuuden odotetaan kuitenkin kasvavan nopeasti. Vuonna 2003 IP-puhelujen osuuden arvioidaan olevan noin kuusi prosenttia kaikista puheluista (Piper Jaffray 1999). Avoin kysymys ei olekaan niinkään IP-puheluiden suosion kasvu vaan se, mikä signaalointiprotokollista vie kisassa voiton. H.323-protokollalla on selvä etumatka – se on toteutettu jo sadoissa tuotteissa ja monet suuret tietoliikenne- ja tietotekniikkayritykset ovat asettuneet tukemaan standardia. Näin on tapahtunut lähinnä sen takia että H.323:lle ei ole aikaisemmin löytynyt todellista vaihtoehtoa.

## Session Initiation Protocol (SIP)

Mutta mitä protokollaa käytetään huomispäivän IP-puheluverkoissa? Onko se H.323, viekö SIP huomattavasti yksinkertaisempaa ratkaisuna voiton pitkällä tähtäimellä vai kehitetäänkö vielä täysin uusi protokolla, kenties kahden edellisen yhteensulautuma? Vai löytävätkö molemmat protokollat omat erilliset käyttöalueensa? On ehdotettu, että H.323 voisi pysyä intranettien protokollana, mihin se on alunperin suunniteltukin ja SIPiä käytettäisiin yleisessä Internetissä, mihin se puolestaan paremmin soveltuu (Bejar 1998).

## Viitteet

### **Handley et al. 1999**

Mark Handley, Henning Schulzrinne, Eve Schooler, Jonathan Rosenberg: "SIP: Session Initiation Protocol", March 1999. Internet Engineering Task Force Request for Comments (Proposed Standard), RFC 2543.

URL: <http://www.ietf.org/rfc/rfc2543.txt>

### **Beijar 1998**

Nicklas Beijar: "Signaling Protocols for Internet telephony", 1998. Helsinki University of Technology.

URL: <http://keskus.hut.fi/tutkimus/ipana/paperit/sip.pdf>

### **Fingal & Gustavsson 1999**

Fredrik Fingal, Patrik Gustavsson: "A SIP of IP-telephony", August 1999. Masters Thesis, Lund Institute of Technology, Lund University.

URL: [http://www.cs.columbia.edu/~hgs/sip/drafts/Fing9902\\_SIP.pdf](http://www.cs.columbia.edu/~hgs/sip/drafts/Fing9902_SIP.pdf)

### **Huovinen & Niu 1999**

Lasse Huovinen, Shuanghong Niu: "IP Telephony", May 1999. Proceedings of the HUT Internetworking Seminar May '99, Helsinki University of Technology.

URL: <http://www.tcm.hut.fi/Opinnot/Tik-110.551/1999/papers/04IPTelephony/voip.html>

### **Lennox et al. 1999**

Jonathan Lennox, Henning Schulzrinne and Thomas F. La Porta: "Implementing Intelligent Network Services with the Session Initiation Protocol", January 1999. Columbia University Computer Science Technical Report CUCS-002-99.

URL: <http://ftp.cs.columbia.edu/reports/reports-1999/cucs-002-99.ps.gz>

### **Mine 1998**

Hilary Mine, Probe Research Inc. "White paper: The Future of Online Communication", October 1998.

URL: [http://www.ap.att.com/countries/telecom/white\\_papers/ipt\\_evolution.doc](http://www.ap.att.com/countries/telecom/white_papers/ipt_evolution.doc)

**Perkins 1996**

C.Perkins: "IP mobility support", October 1996. Internet Engineering Task Force Request for Comments (Proposed Standard), RFC2002.

URL: <http://www.ietf.org/rfc/rfc2002.txt>

**Piper Jaffray 1999**

U.S Bancorp Piper Jaffray (news release): "IP TELEPHONY TO DRIVE THE OPEN COMMUNICATIONS REVOLUTION, ACCORDING TO PIPER JAFFRAY STUDY 2/8/99", February 1999.

URL: [http://www.piperjaffray.com/secaccounts/intranet/newsreleases/pj\\_news135.htm](http://www.piperjaffray.com/secaccounts/intranet/newsreleases/pj_news135.htm)

**Schulzrinne & Rosenberg 1998**

Henning Schulzrinne and Jonathan Rosenberg: "SIP call control services" , November 1999. Internet Draft, Internet Engineering Task Force. Work in progress.

URL: <http://www.ietf.org/internet-drafts/draft-ietf-mmusic-sip-cc-01.txt>

**Wedlund & Schulzrinne 1999**

Elin Wedlund and Henning Schulzrinne: "Mobility Support using SIP", August 1999. Second ACM/IEEE International Conference on Wireless and Mobile Multimedia (WoWMoM'99), Seattle, Washington, August, 1999.

URL: [http://www.cs.columbia.edu/~hgs/papers/Wed19908\\_Mobility.pdf](http://www.cs.columbia.edu/~hgs/papers/Wed19908_Mobility.pdf)

**Muita SIP-linkkejä:**

<http://www.cs.columbia.edu/~hgs/sip/>

<http://www.dynamicsoft.com>

<http://www.bell-labs.com/project/sip>

<http://www.pingtel.com>

<http://www.ietf.org/html.charters/sip-charter.html>