

Siirtyminen perinteisestä
puhelinvaihderyjjestelmästä VoIP-
järjestelmään



Ahonen, Pasi

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Siirtyminen perinteisestä puhelinvaihdejärjestelmästä VoIP-järjestelmään

Pasi Ahonen
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Marraskuu 2009

Pasi Ahonen

Siirtyminen perinteisestä puhelinvaihejärjestelmästä VoIP-järjestelmään
Vuosi 2009 Sivumäärä 49

Tässä opinnäytetyössä käsitellään siirtymistä perinteisestä puhelinvaihejärjestelmästä Voice over Internet Protocol -järjestelmään (VoIP). Opinnäytetyö on tehty hankkeistettuna Fujitsu Services Oy:lle, ja lähtökohtana on suomalaisen kuntayhtymän siirtyminen VoIP-järjestelmään. Opinnäytetyön tekijä toimi harjoittelussa Fujitsulla tuotteistaen ja testaten erilaisia VoIP-järjestelmän laitteita sekä analogilaitteiden liittämistä VoIP-ympäristöön.

Opinnäytetyön alussa esitellään työn lähtökohdat sekä kartoitetaan tilanne rajauksineen. Toisessa luvussa käydään läpi VoIP-tekniikoita ja niiden käyttötapoja ja puheluiden muodostumista teoreettisesti protokollatasolla. Lisäksi osassa avataan VoIP-tekniikkaa sekä siihen liittyviä tietoturvariskejä.

VoIP-järjestelmäosassa esitellään järjestelmien kokoonpano sekä ohjelmisto- että laitteisto-kokoonpanot. Tässä osassa käydään myös läpi mobiili- ja analogilaitteiden liittäminen VoIP-järjestelmään.

Toteutusosassa esitellään kuntayhtymän vanhan IT-infrastruktuurin hyödyntäminen ja se miten VoIP-järjestelmä toteutettaisiin. Tässä osassa käydään läpi fyysinen järjestelmä sekä käyttöliittymät päätelaitteineen.

Lopuksi opinnäytetyö arvioidaan Fujitsun ja kirjoittajan toimesta. Tässä on käytetty hyödyksi Fujitsu Services Oy:ltä saatua asiantuntija-arviota.

Lähdemateriaalina opinnäytetyössä on käytetty kuntayhtymän tarjouspyyntöä, Fujitsun puhepalveluiden palvelukuvausta, VoIP-kirjallisuutta ja Internet-lähteitä.

Pasi Ahonen

Transition from a traditional telephone exchange system to a VoIP-system

Year

2009

Pages

49

The subject of this thesis is a transition from a traditional telephone exchange system to a Voice over Internet Protocol system (VoIP). The thesis has been completed as a project for Fujitsu Services Oy. The baseline has been the transition of a Finnish municipality from traditional telephone exchange system to the VoIP system. The writer of the thesis was as in internship at Fujitsu productizing and testing the various devices of VoIP system.

The initial section of the thesis is the introduction of the baseline and the survey of the situation with the definitions. The second section examines the VoIP technologies and the utilization of VoIP. The second section also describes the building up of the calls and the data security risks talked over.

In the VoIP systems section the configuration, both software and hardware is introduced. This section also describes the merging of the mobile and analog devices to the VoIP system.

The implementation section of the thesis presents the utilization of the municipality's present data infrastructure and an example of how the transition could be carried out. This section explains the physical system and the user interfaces with the terminal.

In the end the thesis is evaluated by the representative of Fujitsu and the writer. The pronouncement of a Fujitsu specialist is used in the evaluation.

The municipality's request for quotation, a service description of the voice services of Fujitsu, technical VoIP-literature and internet sources have been used as the sources for the thesis.

Key words: Voice over Internet Protocol (VoIP), telephone exchange, transition

SISÄLLYS

1	JOHDANTO.....	7
1.1	Lähtökohdat ja tilanteen kartoitus	8
1.2	Opinnäytetyön tavoitteet ja tarkoitus.....	10
1.2.1	Opinnäytetyön tavoitteet	10
1.2.2	Opinnäytetyön tarkoitus.....	11
1.3	Opinnäytetyön ja VoIP-järjestelmätarjouksen rajaukset	12
1.4	Opinnäytetyön ja tarjouksen merkitys asiakkaalle ja Fujitsu Services Oy:lle .	12
2	PERUSTIETOA VOIP:STA	13
2.1	Mitä VoIP tarkoittaa?	13
2.2	Miten VoIP toimii?.....	13
2.3	Miten VoIP toteutetaan, käytötapoja?.....	13
2.3.1	Vertaispalvelut	14
2.3.2	Internet-liittymästä riippumattomat kaupalliset palvelut.....	14
2.3.3	Laajakaistaoperaattorin tarjoamat palvelut.....	14
2.3.4	Asiakasorganisaation sisäinen käyttö.....	14
2.3.5	Operaattorin sisäinen käyttö	15
2.4	VoIP tekniikat ja standardit	15
2.4.1	Signalointi.....	15
2.4.2	Puheen siirto.....	15
2.4.3	Yhdysliikenne	16
2.5	Kuinka VoIP puhelu muodostuu?	17
2.5.1	Puhelun muodostuminen H.323 protokollaa käyttäen.....	17
2.5.2	Puhelun muodostaminen SIP protokollaa käyttäen (Proxy)	20
2.5.3	Puhelun muodostaminen SIP protokollaa käyttäen (Gateway)	22
2.6	Missä VoIP:ia käytetään?.....	24
2.7	Miksi VoIP:ia käytetään?	24
2.8	VoIP ja tietoturva	24
2.8.1	VoIP: Esimerkkejä hyökkäyksistä.....	24
2.8.1.1	Palvelunestohyökkäys.....	24
2.8.1.2	Man-in-the-Middle -hyökkäys.....	25
2.8.1.3	Toisto ja Leikkaa ja liimaa -hyökkäykset	25
2.8.1.4	Palvelun varastaminen	25
2.8.1.5	Salakuuntelu	25
2.8.1.6	Toisena esiintyminen	25
2.8.1.7	Poisoning Attack -hyökkäys.....	25
2.8.1.8	Tunnusten ja henkilöllisyyden varastaminen	26
2.8.1.9	Uudelleenohjaus ja kaappaaminen.....	26

	2.8.1.10 Istunnon keskeyttäminen	26
	2.8.2 Hyökkäysmenetelmiä.....	26
	2.8.3 Palomuurit ja VoIP.....	27
	2.8.4 H.323 signalointisuojaus käyttäen H.235 protokollaa	28
	2.8.5 SIP-signalointisuojaus	28
	2.8.6 Secure RTP	29
	2.8.7 PSTN-yhdyskäytävän suojaus	30
	2.8.8 Yhdyskäytävän turva-arkkitehtuuri	31
	2.8.9 Yhdyskäytävätyypit	31
	2.8.10 Yhdyskäytävät ja soittajatunniste.....	31
	2.8.11 Soittajatunniste ja yksityisyys	32
	2.8.12 Yhdyskäytävän dekomponointi.....	32
	2.8.13 SIP/ISUP-välinen toiminta	32
	2.8.14 Puhelinnumeroiden kartoittaminen DNS:ssä.....	33
	2.8.15 VoIP ja hätäpuhelut.....	33
3	VOIP-JÄRJESTELMÄT	34
	3.1 VoIP-järjestelmien laitteistokokoonpano	34
	3.1.1 Kuluttajasovellukset (järjestelmät)	34
	3.1.2 Yrityskäyttöön soveltuvat järjestelmät	34
	3.1.2.1 Päätelaitteet	34
	3.1.2.2 PSTN-yhdyskäytävät.....	35
	3.1.2.3 Yhdyskäytävät.....	35
	3.1.2.4 Reitittimet.....	36
	3.1.2.5 Palomuurit ja reitittävät palomuurit	36
	3.1.2.6 Palvelimet	36
	3.1.2.7 Ohjelmistot.....	37
	3.2 Mobiililaitteiden liittäminen VoIP-järjestelmään.....	38
	3.3 Analogilaitteiden liittäminen VoIP-järjestelmään.....	40
	3.3.1 Yksittäisten analogilaitteiden liittäminen (VoIP-sovitin)	41
	3.3.2 Useiden analogilaitteiden liittäminen (Mediayhdyskäytävä)	41
4	TOTEUTUS	43
	4.1 Vanha infrastruktuuri ja sen hyödyntäminen.....	43
	4.2 Fyysinen järjestelmä	43
	4.3 Käyttöliittymät ja päätelaitteet.....	43
	4.4 Puhelunvälitys	44
	4.5 Mobiililaitteiden liittäminen VoIP-järjestelmään.....	44
	4.6 Analogilaitteiden liittäminen VoIP-järjestelmään.....	44
5	HANKKEEN ARVIOINTI.....	45
	Lähteet.....	47

Kuvat.....	49
------------	----

1 JOHDANTO

Tämä opinnäytetyö on toteutettu hankkeistettuna Fujitsu Services Oy:lle, ja sen lähtökohtana on erään suomalaisen kuntayhtymän Fujitsulle tekemä tarjouspyyntö koskien siirtymistä perinteisestä puhelinvaihejärjestelmästä VoIP-järjestelmään. VoIP mahdollistaa puheluliikenteen olemassa olevaa IT-infrastruktuuria hyödyksi käyttäen.

Harjoitteluni aikana Fujitsu Services Oy:llä pääsin osallistumaan VoIP-järjestelmien kehittämiseen sekä VoIP-laitteiden tuotteistamiseen. Opinnäytetyössä hyödynnän näitä kokemuksiani analogilaitteiden liittämässä VoIP-järjestelmään.

Ensimmäisessä luvussa käsitellään lähtökohtia, kuntayhtymän Fujitsulle tekemää tarjouspyyntöä ja kuntayhtymän lähtötilannetta. Tässä osassa myös kartoitetaan tavoite sekä tehdään opinnäytetyön rajaukset.

Toisessa, teorialuvussa, esitellään VoIP:ssa käytettäviä protokollia sekä teoriapohjaisesti VoIP:n toimintaa ja puheluiden muodostumista. Tässä osassa esitellään myös tietoturvas asioita koskien VoIP:ia.

Opinnäytetyön kolmas luku käsittelee VoIP-järjestelmiä, niiden laitteisto- ja ohjelmistokoonpanoja sekä sitä miten eri laitteet liittyvät toisiinsa. Tässä luvussa käsitellään myös analogilaitteiden liittämistä VoIP-järjestelmään. Tässä yhteydessä analogilaitteilla tarkoitetaan perinteisen puhelinjärjestelmän laitteita, kuten esimerkiksi fakseja ja puhelinlaitteita.

Neljännessä luvussa esitetään vaihtoehto hankkeen toteutukselle. Tässä on huomioitu kuntayhtymän tarjouspyynnössä tekemät rajaukset sekä Fujitsun puhelupalveluiden palvelukuvaus.

Lopuksi opinnäytetyössä tehdään yhteenveto käsitellystä aiheesta ja arvioidaan sen toteutuskelpoisuus. Tässä käytetään hyödyksi opinnäytetyöstä Fujitsulta saatua palautetta ja arviointia.

1.1 Lähtökohdat ja tilanteen kartoitus

Lähtökohtana on erään eteläsuomalaisen kuntayhtymän Fujitsu Services Oy:lle tekemä tarjouspyyntö. Tavoitteena on siirtää eteläsuomalaisen seudun kaupungit, kunnat ja kuntayhtymät käyttämään Fujitsun tarjoamaa palvelukokonaisuutta, joka koostuu yhteydet sisältävistä puhelinliikenteen palveluratkaisuista.

Asiakkaan puhelintekniset tietoliikennepalvelut kattavat noin 20 puhelinvaihejärjestelmää, joissa on yhteensä 3 086 alaliittymää sekä 1 727 mobiilikäyttäjää. Puhelinyhteydet on toteutettu operaattorien yleisillä kytkentäisillä puhelinverkoilla (PSTN Public Switched Telephone Network) ja GSM (Global System for Mobile Communications). Puhelinvaihejärjestelmät ovat toteutettu erillisinä järjestelminä, jotka koostuvat eri valmistajien tekniikoista.

Kukin organisaatio on hoitanut puhelunvälityksen omilla resursseillaan, välitys on toteutettu yhdessä kulunvalvonnan ja asiakkaiden ohjauksen kanssa. Puhelunvälitys ei kuulu tarjouspyyntöön, vaan toteutetaan jatkossakin asiakkaan omalla henkilöstöllä. Välityspaikkoja on yhteensä seitsemän. Puhelunvälitys tullaan kuitenkin toteuttamaan Fujitsun tarjoamalla välitysympäristöllä. Kunnalliset toimipisteet jakautuvat seitsemän kunnan maantieteelliselle alueelle.

Järjestelmät ja puhelinpalvelut on hankittu useilta osapuolilta ja nykyiset sopimukset ovat päättyneet tai voimassa toistaiseksi. Kahdella kunnalla oli poikkeuksellisesti voimassa oleva vaihdesopimus 1.12.2008 ja 31.1.2009 asti.

Kunnilla on yhteinen IT-palveluja tuottava liikelaitos, joka hallitsee omaa dataverkkoa. Se tuottaa kaikkien kuntien palvelin-, sovellus- ja työasemien tukipalvelut. Dataverkko rajataan pois tarjouspyynnöstä.

Opinnäytetyön tarkoituksena on tehdä esimerkkitapaus, siirtymisestä perinteisestä puhelinvaihejärjestelmästä VoIP-järjestelmään, Fujitsun käyttöön. Asiakkaan näkökulmasta suurin tarve kehittämistoiminnalle on laitteiston ajan tasalle saattaminen sekä kustannuspoliittinen.

Asiakkaan nykyinen puhelinvaihejärjestelmä koostuu erillisistä järjestelmistä, jotka on rakennettu useista erilaisista komponenteista. Laitteista osan valmistus ja tuki on jo lopetettu.

Kunkin kunnan alueella on oma, jokaisen tilaajaosapuolen itsenäisesti hallinnoima puhelinliikenneympäristönsä. Tekniikka on pääosin vanhentunutta.

Osa järjestelmän laitteistosta on asiakkaan omistamaa, ja osa vuokrattu kolmansilta osapuolilta. Asiakkaan eri organisaatiot toimivat laaja-alaisessa yhteistyössä, jota on tarkoitus tiivistää tulevaisuudessa.

Asiakkaan nykytila on seuraavanlainen:

Organisaatio:	Lanka	Mobiili	Yhteensä	Mobiili %	Järjestelmä
xxx kaupunki	380	275	655	42	DIXI Mikko 2000
xxx kunta	250	100	350	29	vuokra
xxx kunta	155	65	220	30	vuokra
xxx kunta	49	35	84	42	
xxx kaupunki	803	390	1193	33	DIXI 700
xxx kaupunki	407	264	671	39	Siemens Hicom 100E 2 kpl
xxx kunta	197	115	312	37	vuokra
xxx seudun kuntayhtymä	220	180	400	45	Dixie BusinessPhone 200, Hicom
xxx xxx ky	467	251	718	35	Meridian Optio 11C
xxx xxx ky	23	2	25	8	Siemens Hicom 100E
xxx xxx ky	135	50	185	27	DIXI 700/900
Yhteensä:	3086	1727	4813	ka 33,36	

Kuva 1: Asiakkaan nykytila. (Muokattu Xxx seudun kuntayhtymä 2007)

Edellä mainitut puhelinvaihejärjestelmät lunastetaan asiakkaalta. Lunastukseen kuuluvat sekä järjestelmät että puhelimet.

Liittymästä ulospäin suuntautuvan liikenteen määrä liittymää kohden on keskimäärin:

- puheluja 120 min/kk eli 1440/v
- puheluja 40 kpl/kk eli 480 kpl/v

Puhelinliikenteestä puolet on paikallista lankaliikennettä, 40 % mobiili-liikennettä, ja 10 % kotimaan kaukoliikennettä.

Mobiili-liikenteestä puolet kohdistuu kotimaisille operaattoreille ja puolet paikalliseen lanka-verkkoon. Tekstiviestejä lähetetään 10 viestiä liittymää kohden kuukaudessa. Ulkomaanliikennettä ei huomioida, koska se on kokonaisuudessaan vähäistä.

1.2 Opinnäytetyön tavoitteet ja tarkoitus

Tässä luvussa käydään läpi opinnäytetyön tavoitteet sekä tarkoitus, kenelle opinnäytetyö on suunnattu ja miksi se kirjoitetaan.

1.2.1 Opinnäytetyön tavoitteet

Opinnäytetyön tavoitteena on mallintaa palveluratkaisu, joka täyttää asiakkaan tarpeet sekä odotukset. Asiakas haluaa palveluratkaisun, joka perustuu ns. yhden puhelimen käyttöön käyttäjäryhmillään.

Käyttäjäryhmiä ovat:

- a) Kiinteästi paikallaan olevat henkilöt ja toiminnot, joiden käytössä on kiinteä VoIP-puhelinliittymä.
- b) Liikkuvat työryhmät ja henkilöt, joiden käytössä on GSM-liittymä.
- c) Erityisryhmät jotka tarvitsevat johtaja-sihteerin ominaisuuksia ja vastaajaryhmiä (käytössään toiminnepuhelin, jolla hallitaan puhelujonoja).

Ratkaisun tavoitteena on kattaa puhelinliikenteen palvelut sisältäen lanka- ja gsm-liittymät, vaihdejärjestelmä ratkaisusta, välityslaitteistot ja liikenne. Ratkaisun tulee olla operaattorin palvelutuote. Asiakas haluaa uudistaa xxxxxx seudun kaupunkien, kuntien ja kuntayhtymien puhutietoliikenteen ja siihen liittyvien palveluiden infrastruktuurin. Opinnäytetyön tarkoituksena on luoda esimerkki tarjottavasta laitteisto- ja ohjelmistokokonaisuudesta.

Kokonaisratkaisussa tulee ottaa huomioon, että se palvelee asiakkaan henkilökuntaa, sidosryhmiä ja kuntalaisia toiminnallisesti ja että se sopii Fujitsun jo tuotteistettuihin ratkaisuihin sekä palveluihin. Tavoitteena on myös tarjota puhutietoliikenteen järjestelmä, joka muodostaa langattomat - ja VoIP-puhelimet yhdeksi kokonaisuudeksi.

Asiakkaalle tarjottava tavoite on vähentää henkilöillä liittymien aiheuttamia kustannuksia tarjoamalla joko yhden tai kahden liittymän ratkaisuja. PSTN-liittymät korvataan VoIP-liittymillä, joko Wicom / SAP Communication Desktop-sovelluksella tai IP-puhelinlaitteella. Olemassa olevaa tietoliikenneverkkoa hyödynnetään puheen kuljettamiseen

Kuvassa 2 kuvataan asiakkaan tavoitetila:

Organisaatio:	VoIP	Mobiili	Yhteensä	Mobiili %	Järjestelmä
xxx kaupunki	130	370	500	74	
xxx kunta	45	290	335	87	
xxx kunta	30	150	180	83	
xxx kunta	11	53	64	83	
xxx kaupunki	249	692	941	74	
xxx kaupunki	100	400	500	80	
xxx kunta	20	197	217	91	
xxx seudun kuntayhtymä	30	350	380	92	
xxx xxx ky	350	310	660	47	
xxx xxx ky	2	20	22	91	
xxx xxx ky	30	185	215	86	
Tarjouspyynnön vertailuvut	1000	3000	4000	ka 75	Fujitsun tarjoama VoIP - järjestelmä.

Kuva 2: Asiakkaan tavoitetila. (Muokattu Xxx seudun kuntayhtymä 2007)

1.2.2 Opinnäytetyön tarkoitus

Tämän opinnäytetyön tarkoituksena on kuvata siirtyminen perinteisestä puhelinjärjestelmästä VoIP-järjestelmään. Opinnäytetyön näkökulma on palveluntarjoajan tekemä tarjous asiakkaan tarjouspyynnön pohjalta. Opinnäytetyön lähtökohta on asiakkaan nykyinen tilanne sekä järjestelmä. Tavoitteena on VoIP-järjestelmän kuvaus, jonka Fujitsu voisi asiakkaalle rakentaa.

Työssä käytetään aineistona alan kirjallisuutta, ammattijulkaisuja sekä opetustarkoitukseen kirjoitettua materiaalia. Käytän myös omakohtaisia havaintojani analogilaitteiden yhteen liittämistä VoIP-järjestelmien kanssa.

Opinnäytetyö on Fujitsun hankkeistama, joten se kohdistetaan sekä Laurea-ammattikorkeakoululle että Fujitsulle. Tavoitteena on kuvata Fujitsulle palvelukokonaisuus myynnin ja tekniikan käyttöön.

Opinnäytetyössä kuvataan ja selvennetään etenkin analogilaitteiden ja VoIP-järjestelmien yhteen liittämisen monimutkaisuutta sekä järjestelmän vikasietoisuuden parantamista.

Työn keskeisiä termejä tulevat olemaan VoIP-, puhelinjärjestelmä- ja tietoliikenneprotokollat sekä niiden lyhennelmät. Kaikki käytetyt termit tullaan avaamaan opinnäytetyössä.

1.3 Opinnäytetyön ja VoIP-järjestelmätarjouksen rajaukset

Tavoitteena on tehdä Fujitsulle hankkeistettu opinnäytetyö, jonka tarkoituksena on tuottaa materiaalia siirtymisestä perinteisestä puhelinvaihejärjestelmästä VoIP-järjestelmään, Fujitsun käyttöön.

Opinnäytetyöhön ei sisälly siirtymisen toteutus, vaan esimerkkikuvaus siirtymisvaihtoehdosta. Kuntayhtymän nykyisen verkon kartoittaminen ei kuulu opinnäytetyöhön.

Tarjoukseen ei sisälly puheluvälittäjien työ, vaan kuntayhtymä hoitaa sen edelleen omalla henkilöstöllään. Dataverkko ei kuulu tarjouksen piiriin, sillä kunnilla on oma yhteinen IT-palveluja tuottava liikelaitoksensa. Kuntayhtymä ei hyväksy osa- tai vaihtoehtoisia tarjouksia.

Kuntayhtymä vastaa itse siitä, että toimeksi annetut tietoliikennejärjestelyt ovat tietoturva- ja politiikan mukaisia sekä tietoturva- ja politiikkansa ylläpitämisestä. Kuntayhtymän käyttämät laitteet tai ohjelmistot eivät saa aiheuttaa haittaa tai häiriötä palvelun toimittajalle eivätkä muille yhdysliikennepisteen käyttäjille.

1.4 Opinnäytetyön ja tarjouksen merkitys asiakkaalle ja Fujitsu Services Oy:lle

Opinnäytetyöllä ei ole suoraa merkitystä kuntayhtymälle, opinnäytetyön pohjalta voidaan vasta laatia tarjous asiakkaalle.

Opinnäytetyö tarjoaa Fujitsulle materiaalia sisäiseen käyttöön, vastaavia projekteja varten. Materiaalia VoIP-järjestelmien kokoonpanoratkaisuista sekä teknologioista voidaan hyödyntää myynnin ja projektihenkilöstön käytössä.

2 PERUSTIETOA VOIP:STA

Luvussa käydään läpi VoIP:n perustietoja ja käyttöä, avataan eri protokollia sekä selvennetään miten VoIP toimii. Lisäksi luvussa käsitellään tietoturva-asioita.

2.1 Mitä VoIP tarkoittaa?

VoIP (Voice over Internet Protocol) tarkoittaa nimensä mukaisesti internet-protokollan päällä kulkevaa ääntä. Ääni kulkee tässä tapauksessa datapaketteina, TCP- (Transmission Control Protocol) ja UDP-protokollien välityksellä (User Datagram Protocol) dataverkossa. (Liikenne- ja viestintäministeriö 2005, 1-3)

VoIP:lla tarkoitetaan siis internetissä, IP-paketteina eli datamuodossa, kulkevaa puhetta. VoIP:sta puhuttaessa viitataan myös usein protokolliin sekä internetpuheluiden mahdollistaviin tekniikoihin sekä teknologioihin.

2.2 Miten VoIP toimii?

VoIP-puhelut muodostuvat joko erillisten LAN-verkkoon (Local Area Network) kytkettyjen VoIP-puhelinlaitteiden tai tietokoneeseen liitettyjen IP-puhelinlaitteiden välityksellä. IP-puhelimet toimivat kuten tavalliset PSTN-verkkoon (Public Switched Telephone Network) päätelaitteet. Tietokoneeseen liitettävät IP-puhelimet vaativat toimiakseen erityisen sovelluksen, tavallisin kuluttajasovellus lienee Skype. Puhelu välittyy dataverkossa Internet-protokollan (IP) välityksellä.

Saman LAN-verkon sisällä soitetut puhelut välittyvät kytkimien välityksellä MAC-osoitteiden (Media Access Control) perusteella. Jos puhelu soitetaan LAN-verkon ulkopuolelle, tarvitaan reitintä, joka reitittää IP-paketit oikealle vastaanottajalle IP-osoitteen perusteella.

VoIP-liikenteen IP-paketeissa siirretään sekä TCP- että UDP-paketteja. VoIP-paketit ovat pääsääntöisesti yhteydettömään UDP:hen perustuvaa liikennettä. VoIP-sovellus lähettää myös TCP-paketteja puhelun aikana, mutta itse puhe kulkee UDP-paketteina. (Liikenne- ja viestintäministeriö 2005, 3).

2.3 Miten VoIP toteutetaan, käyttötapoja?

Euroopan komissio on VoIP-raportissaan jakanut VoIP-palvelut viiteen ryhmään. Viestintä- ja liikenneministeriö on vapaasti suomentanut luokittelun, jota käytetään myös tässä opinnäytetyössä.

2.3.1 Vertaispalvelut

Vertaispalveluja ovat VoIP-palvelut, joista ei muodostu puhelumaksuja ja jotka toimivat avoimessa internetissä. Vaatimuksena on Internet-yhteys sekä IP-puhelut mahdollistava sovellus. Tunnetuimpia sovelluksia ovat Windows Live Messenger, ennen Microsoft Messenger (Windows Live Messenger 2008) ja Skype (www.skype.com 2008).

2.3.2 Internet-liittymästä riippumattomat kaupalliset palvelut

VoIP-palvelut ovat riippumattomia verkkopalvelun tarjoajasta ja niinpä käyttäjä voi vapaasti valita myös jonkun muun palveluntarjoajan kuin oman internet palveluntarjoajansa, ISP:nsä (Internet Service Provider). Esimerkiksi helsinkiläinen Cuuma Communications Oy toimii VoIP-palveluntarjoajana. (www.cuuma.com 2008).

Internet-liittymästä riippumaton VoIP-palveluntarjoaja ei kuitenkaan pysty takaamaan palvelun laatua QoS (Quality of Service), tämä todetaan myös Euroopan komission VoIP -raportissa. (Liikenne- ja viestintäministeriö 2005, 15).

2.3.3 Laajakaistaoperaattorin tarjoamat palvelut

Kuluttajakäytössä on yleistymässä malli, jossa ISP tarjoaa myös VoIP-palvelun asiakkaalleen. Tämän etuna on se, että operaattori pystyy valvomaan puheen siirrolle tarvittavan palvelun laadun. Operaattoreista tunnetuimpia ovat SW television Oy /Welho (Tietoa Welhosta 2008) ja Saunalahti Group Oyj (Nettipuhelin 2008).

Welho tarjoaa puhelut kiinteään kuukausihintaan ja Saunalahti käyttää aikaperusteista hinnoittelua.

2.3.4 Asiakasorganisaation sisäinen käyttö

Valtaosa suurista organisaatioista käyttävät VoIP-järjestelmiä, motiiveina ovat kustannusten säästö sekä IP-tekniikan tuomat toiminnalliset hyödyt. (Liikenne- ja viestintäministeriö 2005, 18).

Suurissa organisaatioissa myös laitetekniset säästöt korostuvat, kun organisaatioiden ei tarvitse hankkia tai vuokrata kalliita puhelinvaihejärjestelmiä ja niiden ylläpitoa. Joissain organisaatioissa, joissa puhelinvaihejärjestelmä on toteutettu PSTN-tekniikkaa käyttäen, ollaan jo tilanteessa, jossa puhelinvaihejärjestelmät ovat teknisesti vanhentuneita eikä niihin ole enää tukea saatavissa.

2.3.5 Operaattorin sisäinen käyttö

Viestintä- ja liikenneministeriön vuonna 2005 tekemän selvityksen mukaan operaattorit ovat käyttäneet VoIP:ia puhelinverkon sisäisenä tekniikkana jo 1990-luvulta lähtien. Pääasiallisena syynä tähän on kustannussäästöt erityisesti ulkomaanpuheluissa. TDC Oy (entinen TDC Song, Song Networks ja Telia Finland) aloitti VoIP:n käytön ulkomaanpuheluissa, 994-puheluissaan.

2.4 VoIP tekniikat ja standardit

VoIP:n toteuttamiseen liittyvät tekniikat ja standardit voidaan jakaa neljään osaan. Ne ovat signalointi (merkinanto), puheen siirto, yhdysliikenne ja liikkuvuuden tuki. (Liikenne- ja viestintäministeriö 2005, 23).

2.4.1 Signalointi

Signaloinnilla tarkoitetaan tapaa, jolla IP-puhelu muodostetaan, sitä hallitaan ja se puretaan. Yhteys puhelun osapuolten kesken muodostetaan pyytämällä tiedetystä IP-osoitteesta lupaa yhteydelle. VoIP:n signaloinnissa käytetään SIP (Session Initiation Protocol) ja H.323 protokollia.

SIP ja H.323 käyttävät sähköpostin omaisia osoitteita, ja molempia voidaan käyttää sekä IP-puheluissa että videoneuvotteluissa. SIP on kuitenkin syrjäyttämässä H.323:n, sillä SIP on huomattavasti helpommin integroitavissa IP -puheluiden ja muiden sovellusten välillä. (Liikenne- ja viestintäministeriö 2005, 28).

2.4.2 Puheen siirto

Puheen siirto voidaan jakaa palvelunlaatuun (QoS), koodaukseen, reititykseen ja palomuurin läpäisyyn.

Palvelunlaatuun vaikuttavia tekijöitä ovat kapasiteetti, joka VoIP-sovelluksella on käytettävissä (kbit/s), jitter eli pakettien viive ja viiveen vaihtelu sekä pakettien katoamistodennäköisyys.

VoIP-puhelut siirretään digitaalisessa muodossa ja siksi puhe täytyy digitoida ja koodata siirtoa varten. Yleisimmät käytetyt koodaus- ja dekodeustavat ovat G.711, G.723.1 u/A, G.729 ja iLBC.

Reitityksessä käytetään IPv4 ja IPv6 Internet-protokollia. IPv4 on laajasti käytössä USA:ssa ja Länsi-Euroopassa, kun taas lähes kaikki Kiinan ja Japanin VoIP-palvelut kehitetään IPv6:n.

Tämä johtuu siitä, että IPv4-osoitteet (noin 4 miljardia osoitetta yhteensä) on jaettu pääsääntöisesti USA:n ja Länsi-Euroopan maiden käyttöön. NAT (Network Address Translation) on myös vähentänyt osoitteiden tarvetta.

Jotta VoIP -puhelut voidaan reitittää LAN:n ulkopuolelle, tarvitaan porttiavauksia palomuurin. VoIP:n käyttämän UDP portit tulee avata VoIP-liikenteelle. Palomuuressa on yleisesti käytössä dynaaminen pakettisuodatus ja sovellustason yhdyskäytävät. (Liikenne- ja viestintäministeriö 2005, 23-34).

2.4.3 Yhdysliikenne

Yhdysliikenne voidaan jakaa kahteen eri osa-alueeseen, yhdysliikenteeseen VoIP-järjestelmien välillä ja yhdysliikenteeseen PSTN-verkkoon.

Uudet VoIP-operaattorit käyttävät järjestelmiensä välillä VoIP peering käytäntöä. Siinä operaattorit liittävät järjestelmänsä yhteen ilman keskinäistä laskutusta.

Perinteiset puhelinoperaattorit soveltavat VoIP:ia perinteisiin yhdysliikennejärjestelyihinsä ja soveltavat perinteisiä laskutusmallejaan.

Yhdysliikenteessä PSTN-verkon kanssa puhelinnumerot muunnetaan domain-nimiksi, jollaisina ne tallennetaan DNS:n (Domain Name Service) eli Internetin nimipalvelimeen. Tässä käytetään ENUM (Electoric Numbering) tekniikkaa. Se on IETF:n (Internet Engineering Task Force) kehittämä tapa muuntaa puhelinnumero URI:ksi (Universal Resource Identifier).

VoIP asettaa haasteita liikkuvuuden tuelle, päätelaitteen tulisi pystyä siirtymään fyysisestä verkosta ja tukiasemasta toiseen ilman, että VoIP-puhelu katkeaa.

Kehitteillä on VoWLAN (Voice over Wireless Local Area Network) palveluita, tällä hetkellä ongelma syntyy päätelaitteen rekisteröityessä tukiasemalta toiselle kesken puhelun. (Liikenne- ja viestintäministeriö 2005 35-37).

Esimerkiksi Cisco on kehittänyt jo langattomia tukiasemia, jotka vähentävät puheluiden katkeamista rekisteröidytessä tukiasemasta toiseen. Tämä perustuu verkkovierailun nopeampaan siirtämiseen. (Wireless-Nets, Ltd 2008).

2.5 Kuinka VoIP puhelu muodostuu?

Seuraavissa kappaleissa käydään läpi puhelun muodostumista kahta eri protokollaa käyttäen. Yhteistä puhelun muodostamiselle on yhteyden muodostamisessa käytettävät TCP-sanomat sekä puheen siirtäminen UDP-paketteina. Itse viestit eroavat toisistaan, ja ne kuvataan seuraavissa kappaleissa.

OSI -MALLI	PROTOKOLLAT	TCP/IP -MALLI
7. SOVELLUSKERROS	H.323, SIP, DHCP, DNS, FTP, IMAP4, POP3	4. SOVELLUSKERROS
6. ESITYSTAPAKERROS	GIF, JPG, MPEG	
5. ISTUNTOKERROS	H.245, NetBIOS, PPTP, RTCP, SSH	
4. KULJETUSKERROS	TCP, UDP, RTMP	3. KULJETUSKERROS
3. VERKKOKERROS	IPv4, IPv6, ICMP, IGMP, IPsec, RIP, Reititin	2. VERKKOKERROS
2. SIIRTOKERROS	ATM, Ethernet, IEEE 802.2 / 11, PPP, STP	1. PERUSKERROS
1. FYYSINEN KERROS	Verkkokortti, Toistin, Kytin, Modeemi, V.92 modeemi, ISDN, T1, E1	

Kuva 3: OSI- ja TCP/IP -mallin kuvaus. (Muokattu Kaario 2002)

2.5.1 Puhelun muodostuminen H.323 protokollaa käyttäen

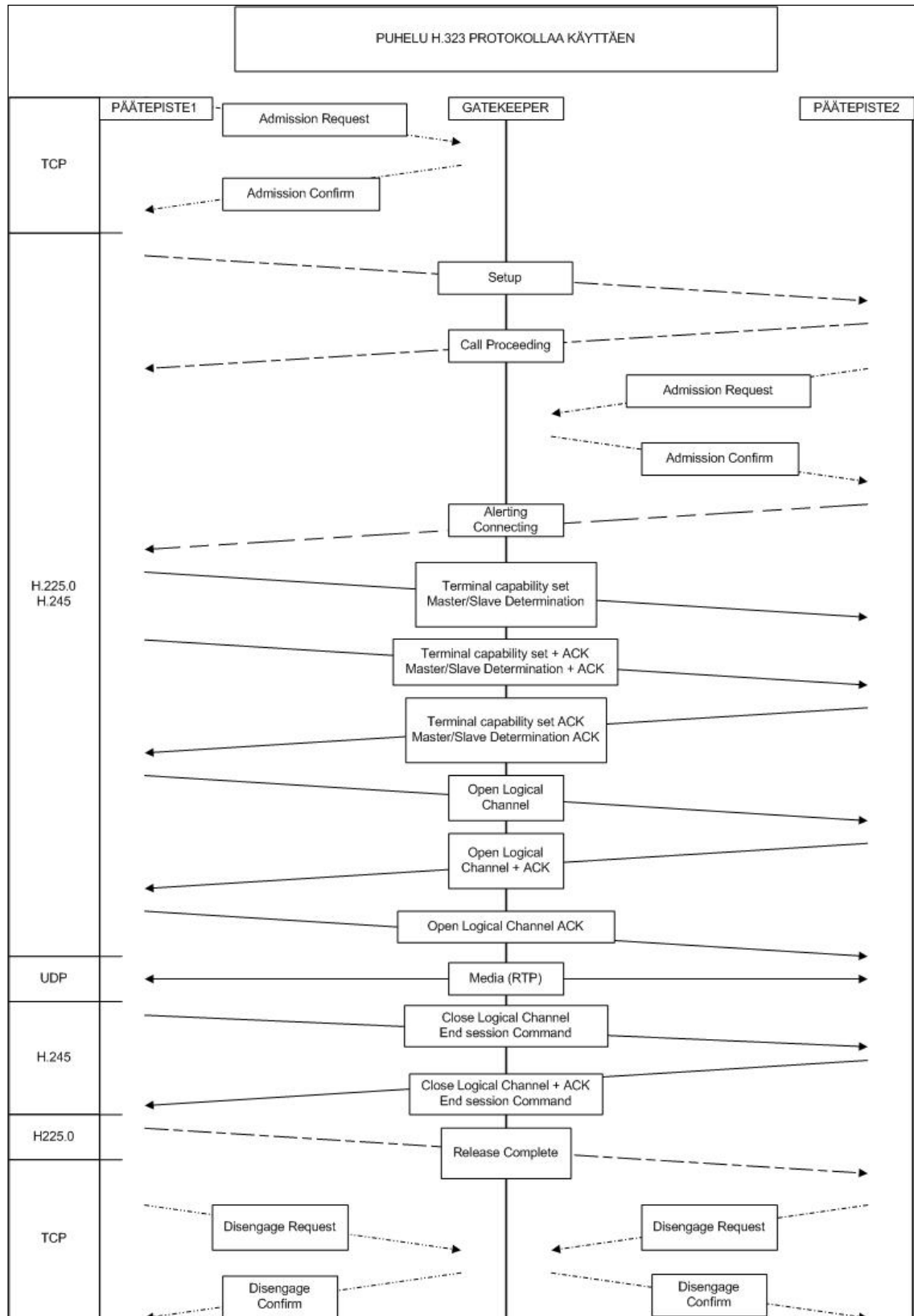
Puhelun muodostaminen voidaan jakaa neljään vaiheeseen, vaiheiden erot saattavat olla epäselviä johtuen käytettävästä signaalintimallista.

Vaiheessa 1 puheluyhteys muodostetaan. Jotta puhelu voidaan muodostaa, täytyy muodostaa luotettava yhteys päätepisteeseen TCP:llä tai Välityspalvelimena (Proxy) toimivan gatekeeperin välityksellä. Puhelun alussa lähetetään yhteydenmuodostuspyyntö (SYN) TCP-sanomana. Gatekeeper vastaa yhteydenmuodostuskuittauksella, TCP-sanoma (ACK).

Vaiheet 2-4 ovat loogisen kanavan - ja lisäpalveluiden kontrollointisignaaleja. Seuraavaksi tunneloidaan H.245 yhteys, yhteydessä käytetään H.225 sanomia (Asetus, puhelun käsittely, hälytys ja yhdistys.) Median siirtämistä varten avataan lähettävän ja vastaanottavan UDP-

portin välille yhteys, median siirtämisessä käytetään Real-Time Transmission Protokollaa (RTP).

Puhelun lopettava vaihe 5 koostuu yksinkertaisista merkinannon vaihtamisista, joilla osapuolet ymmärtävät että mediakanavat ovat suljettu ja puhelu päättyy. Sanomat ovat TCP-paketteja. (Sulje looginen kanava, end command -käsky, puhelun katkaiseminen suoritettu, irtikytkeytymispyyntö ja -vahvistus.) (Putting VoIP to Work 2002, 133-160).



Kuva 4: Puhelun muodostaminen H.323 protokollaa käyttäen. (Muokattu Douskalis 2002)

2.5.2 Puhelun muodostaminen SIP protokollaa käyttäen (Proxy)

Jotta puhelu voidaan muodostaa, täytyy muodostaa luotettava yhteys päätepisteiden välille välityspalvelimen (Proxy) kautta.

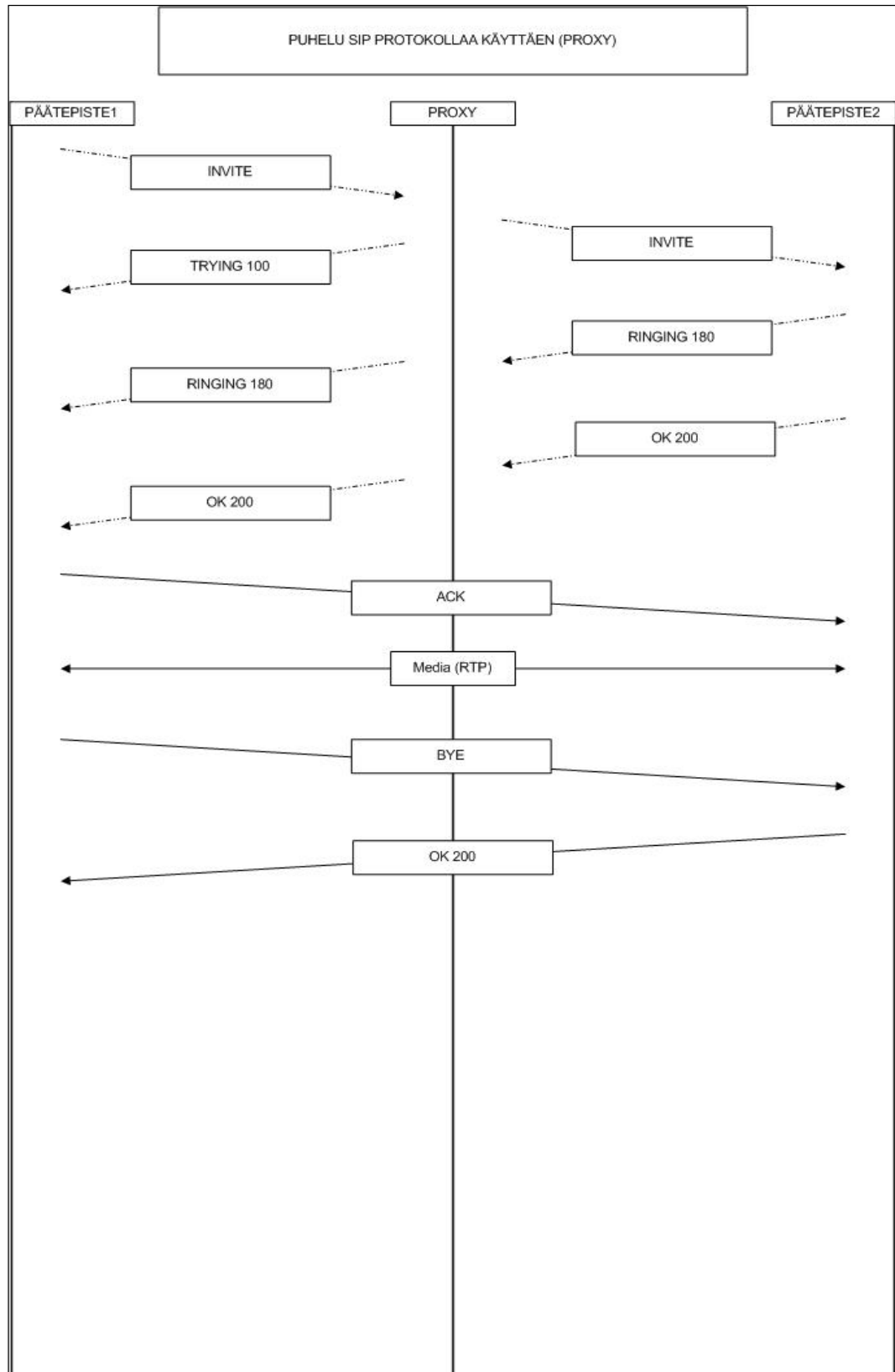
Päätepiste 1 lähettää Proxylle yhteydenmuodostamispyyntön (Invite). Proxy välittää viestin edelleen päätepisteeseen 2, samanaikaisesti päätepiste 1 saa Proxylta viestin Trying koodilla 100.

Päätepiste 2 lähettää Proxylle viestin Ringing koodilla 180, joka välitetään edelleen päätepisteeseen 1.

Päätepiste 2 lähettää Proxylle viestin OK koodilla 200, Proxy välittää viestin päätepisteelle 1. Tämä tarkoittaa käytännössä, että yhteydenmuodostuspyyntö on suoritettu onnistuneesti.

Päätepiste 1 lähettää päätepisteelle 2 Proxyn kautta kiittausviestin (ACK). Nyt puhelu voidaan muodostaa päätepisteiden välille. Puhe siirretään käyttäen Real-time Transport Protokollaa (RTP).

Puhelun lopussa päätepiste 1 lopettaessaan puhelua lähettää Proxylle viestin BYE lopettaakseen puhelun. Päätepiste 2 lähettää päätepisteelle 1 kiittauksen OK 200 välityspalvelimen kautta. Puhelu katkeaa, molemmat päätepisteet vapautuvat ja ovat valmiina soittamaan tai vastaanottamaan puheluita. (Putting VoIP to Work 2002, 221-257).



Kuva 5: Puhelun muodostaminen SIP protokollaa käyttäen (Proxy). (Muokattu Douskalis 2002)

2.5.3 Puhelun muodostaminen SIP protokollaa käyttäen (Gateway)

Yhdyskäytävää (Gateway) käytetään silloin, kun liitetään erilaisia verkkoja yhteen. Esimerkiksi yleinen kytkentäinen puhelinverkko (PSTN) ja VoIP-verkko.

Jotta puhelu voidaan muodostaa, täytyy muodostaa luotettava yhteys päätepuhelinlaitteiden välille välityspalvelimen (Proxy) kautta.

Päätepuhelinlaitte 1 lähettää Proxylle yhteydenmuodostamispyyntön (Invite). Proxy kuittaa tämän lähettämällä viestin Trying koodilla 100 päätepuhelinlaitteelle 1. Samalla Proxy lähettää viestin edelleen Gatewaylle, joka välittää puhelunaloituspyyntön PSTN verkkoon, päätepuhelinlaitteelle 2.

Päätepuhelinlaitteessa 2 puhelin alkaa soida, ja Gateway välittää Proxyn kautta päätepuhelinlaitteeseen 1 viestin Ringing koodilla 180.

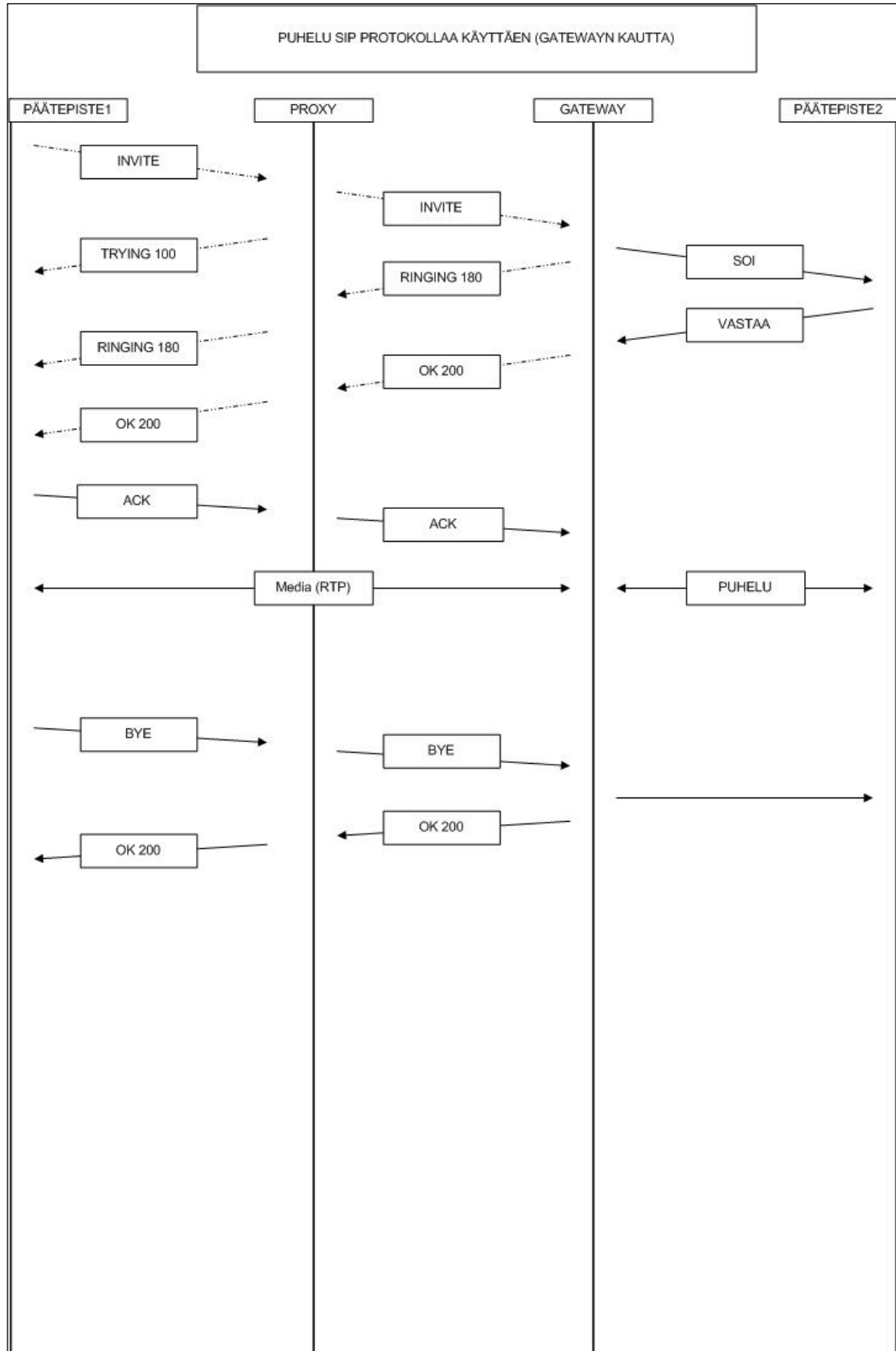
Päätepuhelinlaitteessa 2 vastataan puhelimeen, ja Gateway lähettää Proxyn kautta päätepuhelinlaitteelle 1 viestin OK koodilla 200. Yhteydenmuodostuspyyntö on suoritettu onnistuneesti.

Päätepuhelinlaitte 1 välittää Gatewaylle kuittausviestin (ACK). Puhelu muodostuu päätepuhelinlaitteiden välille. Puhe siirretään päätepuhelinlaitteen 1 ja Gatewayn välillä käyttäen Real-time Transport Protokollaa (RTP).

Gateway välittää puhelun PSTN verkkoon päätepuhelinlaitteelle 2. Vastaavasti päätepuhelinlaitteen 2 puhe välitetään Gatewayn kautta päätepuhelinlaitteelle 1.

Puhelun lopussa päätepuhelinlaitte 1 lopettaessaan puhelua lähettää Proxylle viestin BYE lopettaakseen puhelun. Proxy lähettää viestin edelleen Gatewaylle, joka ilmoittaa PSTN verkkoon päätepuhelinlaitteelle 2 puhelun loppuneen.

Gateway lähettää päätepuhelinlaitteelle 1 kuittauksen OK 200 Proxyn kautta. Puhelu katkeaa, molemmat päätepuhelinlaitteet vapautuvat ja ovat valmiina soittamaan tai vastaanottamaan puheluita. (Putting VoIP to Work 2002, 221-257).



Kuva 6: Puhelun muodostaminen SIP protokollaa käyttäen (Gateway). (Muokattu Douskalis 2002)

2.6 Missä VoIP:ia käytetään?

VoIP:ia ovat alkaneet käyttämään julkishallinnon organisaatiot, yritykset sekä yksityishenkilöt.

Yksityishenkilöillä käyttö muodostuu lähinnä VoIP-sovelluksen, Skype tai Windows Live Messenger käytöstä, ja yrityksillä VoIP-puhelinjärjestelmistä.

2.7 Miksi VoIP:ia käytetään?

Tärkeimmät syyt VoIP:n käyttöön siirtymisessä ovat siirtymisestä aiheutuvat säästöt. Säästöjä saavutetaan puheluissa, laitteistoissa ja etenkin niiden ylläpidossa ja verkonhallinnassa.

Organisaatiot saavuttavat huomattavaa taloudellista hyötyä maksuttomissa sisäpuheluissa, sekä paikallispuhelinhintaissa kauko- ja ulkomaanpuheluissa. Kauko- ja ulkomaanpuhelut siirretään IP-verkossa oikealle teleliikennealueelle ja yhdyskäytävän kautta paikallispuheluina perille. Yrityksillä on yleensä jo valmiit IP-verkkoyhteydet käytössään, joten sisäpuheluiden siirtäminen IP-verkkoon ei vaadi lisäinvestointeja.

2.8 VoIP ja tietoturva

VoIP-liikenne poikkeaa huomattavasti PSTN-verkossa tapahtuvasta puheliikenteestä. PSTN-verkkojen erilainen rakenne mahdollistaa fyysisen suojauksen, jota VoIP-verkossa ei ole. Internet itsessään mahdollistaa salakuuntelun tehokkaasti. Tämän vuoksi tietoturvaratkaisuja on lisättävä, jotta VoIP-liikenteen signaalointia sekä media protokollia voidaan suojata. Tietoturvaohjelmat liittyvät enemmän Internetissä käytettäviin VoIP-palveluihin. Suurin osa voidaan sulkea pois käytettäessä asiakkaalle dedikoituja palveluja ja -yhteyksiä. (Understanding Voice over IP Security 2006,3).

2.8.1 VoIP: Esimerkkejä hyökkäyksistä

Tässä luvussa esitellään hyökkäyksiä, joita voidaan käyttää VoIP-liikennettä vastaan.

2.8.1.1 Palvelunestohyökkäys

Palvelunestohyökkäys (Denial of Service, DoS) tarkoittaa hyökkäystä, jossa verkkopalvelua (isäntäkonetta, kytkintä, reititintä, palvelinta tai sovellusta) ylikuormitetaan joko hidastaakseen tai estääkseen sitä toimimasta. (Understanding Voice over IP Security 2006,51-56).

2.8.1.2 Man-in-the-Middle -hyökkäys

Man-in-the-Middle -hyökkäys (MitM) on perinteinen hyökkäys, jossa hyökkääjä tunkeutuu kahden isäntäkoneen väliin ja reitittää heidän välisen liikenteen kauttaan. Tässä hyökkäyksessä tunkeutuja kykenee tutkimaan ja muuttamaan paketteja sekä lisäämään omia pakettejaan liikenteeseen. Hyökkääjä voi myös estää tiettyjen pakettien liikenteen kokonaan. (Understanding Voice over IP Security 2006, 56-57).

2.8.1.3 Toisto ja Leikkaa ja liimaa -hyökkäykset

Toisto (Reply) ja Leikkaa ja liimaa (Cut-and-Paste) ovat hyökkäyksiä, joissa kaapataan syntaksin vaatimukset täyttävä, validi, paketti. Paketti lähetetään sitten eteenpäin hyötymistarkoituksessa, yleensä esiintyäkseen valtuutettuna käyttäjänä. (Understanding Voice over IP Security 2006, 57-58).

2.8.1.4 Palvelun varastaminen

Palvelun varastaminen alkaa yleensä tunnusten, yhteisten salasanojen tai yksityisten salasanojen varastamisella. (Understanding Voice over IP Security 2006, 58-59).

2.8.1.5 Salakuuntelu

Salakuuntelu on useimmiten vaikea huomata, sillä poikkeavaa liikennettä ei verkossa tapahdu. VoIP-liikenteen salakuuntelu voidaan toteuttaa signaloinnin tai median kuunteluna. (Understanding Voice over IP Security 2006, 59-60).

2.8.1.6 Toisena esiintyminen

Toisena esiintyminen tarkoittaa käyttäjän ja isäntäkoneen tekeytymistä toiseksi käyttäjäksi tai isäntäkoneeksi. Yleensä tarkoituksena on saada tietoon luottamuksellista tietoa, kuten käyttäjätunnuksia, salasanoja sekä verkkopankkitunnuksia. (Understanding Voice over IP Security 2006, 60).

2.8.1.7 Poisoning Attack -hyökkäys

Poisoning Attack tarkoittaa hyökkäystä, joka kohdistetaan Internetin nimipalvelujärjestelmää (Domain Name System, DNS) tai Address Resolution Protocol:ia (ARP) vastaan. Hyökkääjä voi käyttää virusta tai vakoiluohjelmaa muokatakseen juuripalvelimia tai oletusnimipalvelimia

siten, että käyttäjät ohjautuvat hyökkääjän nimipalvelimelle, joka palauttaa virheellisiä ja haitallisia vastauksia DNS-kyselyihin. (Understanding Voice over IP Security 2006, 60-61).

2.8.1.8 Tunnusten ja henkilöllisyyden varastaminen

Tunnusten ja henkilöllisyyden varastaminen auttaa hyökkääjää saamaan hyväksyttävän henkilöllisyyden tai todennustunnukset. Hyökkäystä voidaan käyttää edelleen suorittaakseen muita hyökkäyksiä, kuten palvelun varastamista. (Understanding Voice over IP Security 2006, 61-62).

2.8.1.9 Uudelleenohjaus ja kaappaaminen

Uudelleenohjaus tai kaappaus on hyökkäys, jossa toinen puhelun päätepisteistä vaihdetaan tahallisesti. (Understanding Voice over IP Security 2006, 62-63).

2.8.1.10 Istunnon keskeyttäminen

Istunnon keskeyttäminen tarkoittaa kaikkia niitä hyökkäyksiä, joilla alennetaan tai häiritään käytössä olevaa signalointia, median kulkua tai vahvistamista odottavia istuntoja. (Understanding Voice over IP Security 2006, 63-64).

2.8.2 Hyökkäysmenetelmiä

Tässä luvussa esitellään hyökkäysmenetelmiä, joita voidaan käyttää VoIP-liikennettä vastaan.

Porttiskannaus on menetelmä, jolla pyritään muodostamaan yhteys palvelimen portteihin. VoIP-palvelimet käyttävät tunnettuja portteja, kuten porttia 5060 SIP-protokollalle. Porttiskannaus on nykyään niin laajalle levinnyttä, että tietoturvajohdajien on vaikea päätellä milloin järjestelmät ovat tarkoituksellisesti kohteena. (Understanding Voice over IP Security 2006, 64).

Haitallisella koodilla tarkoitetaan kaikkia ohjelmistoja, jotka ovat asennettu ilman käyttöluppaa, ilmoitusta tai koneen omistajan tai hallinnoijan hyväksyntää. Haitalliset ohjelmistot aktivoituvat yleensä asennuksen jälkeen viruksiksi, madoiksi, vakoiluohjelmiksi tai troijalaisiksi. (Understanding Voice over IP Security 2006, 65).

Puskurin ylivoutaminen on menetelmä, jonka kohteena ovat ohjelmiston lähtöparametrit tai ohjelmistossa oleva arvo, johon vaikuttamalla pyritään aiheuttamaan häiriö. (Understanding Voice over IP Security 2006, 67-68).

Salasanojen hankkiminen voidaan toteuttaa joko varastamalla tai käyttämällä brute-force (raaka voima) -menetelmää, jossa salasanaa syötetään niin kauan kunnes oikea löytyy. (Understanding Voice over IP Security 2006, 69).

Tunnelointi on hyökkäysmenetelmä, jossa yhtä protokollaa ajetaan toisen sisällä, yleensä tarkoituksena on päästä palomuurin ohi. (Understanding Voice over IP Security 2006, 69).

Bid Down tarkoittaa menetelmää, jonka tarkoituksena on saada toisten osapuolien tietoturvas-
tasoa laskettua alemmas. (Understanding Voice over IP Security 2006, 69).

2.8.3 Palomuurit ja VoIP

VoIP asettaa seuraavanlaisia haasteita palomuuureille:

1. VoIP käyttää dynaamisia portteja mediaistuntoihin.
2. Palomuurit tukevat ja tarjoavat verkko-osoitteiden kääntöä (Network Address Translation, NAT), mutta muokatut osoitteet ovat ristiriidassa ja häiritsevät VoIP-signalointia.
3. Useimmat palomuurit eivät ole QoS:ä tukevia.

VoIP:ssa käytettävän palomuurin tulee olla sovellustietoinen ja pystyä käsittelemään VoIP-protokollia sekä tarjoamaan suojaa VoIP:lle ominaisia hyökkäyksiä vastaan.

VoIP-palomuuria valittaessa tulisi ottaa, että se täyttää seuraavat kriteerit:

1. Tukee suojausprotokollaa, joka tarjoaa suojan signalointiin ja median kulkuun. Se tukee päätepisteiden todennusta, viestien ja median salakoodausta sekä suojaa eheyden.
2. Siinä tulee olla VoIP-yhteensopivat NAT- ja porttihakentä.
3. Granular Call Admission (CAC).
4. Edellytykset hallita useita samanaikaisia puheluita (DoS suojaus).
5. Se tarjoaa suojan informaatioprosesseja ja -teknologioita (Information Processes and Technology (IPT) vastaan suunnattuja sovellustason hyökkäyksiä vastaan.
6. Siinä on edellytykset valvoa tavallisesta poikkeavia soittokaavoja.
7. Se mahdollistaa yksityiskohtaisen lokin VoIP:n liittyvistä tapahtumista.
8. Se valvoo ja ylläpitää QoS:a kaikissa mediapaketeissa.
9. Palomuuuri mahdollistaa QoS -merkittyjen mediapaketien käsittelyn, sekä säilyttää merkit kaikessa palomuurin kautta kulkevassa liikenteessä.

(Understanding Voice over IP Security 2006, 92-93).

2.8.4 H.323 signalointisuojaus käyttäen H.235 protokollaa

H.235 protokolla vastaa H.323 protokollan suojauksesta, se tarjoaa suojan seuraaville osille:

1. H.225 Registration Admission Status (RAS) signalointiin päätepisteen ja gatekeeperin välillä.
2. H.225 puhelun signalointiin.
3. H.245 valvontakanavan signalointiin.

H.235 protokolla määrittää myös mediansiirron todentamisen ja salakirjoittamisen käyttäen Secure RTP:tä (SRTP). (Understanding Voice over IP Security 2006, 160-161).

2.8.5 SIP-signalointisuojaus

SIP määrittää useita mekanismeja todentamisen, luottamuksellisuutta sekä eheyden suojaamiseen. (Understanding Voice over IP Security 2006, 146).

HTTP Perustodentaminen määritellään RFC 2543 dokumentissa. Perustodentamisessa käyttäjätunnukset siirretään selkotekstisenä, joten salasana voidaan palauttaa vastausviestistä. Tätä todennustapaa onkin siksi syytä käyttää yhdessä jonkin aikaleiman kanssa, jotta vastaushyökkäyksiltä voidaan suojautua. (Understanding Voice over IP Security 2006, 146).

SIP lainaa tiivistettyä todentamista http-protokollalta, johon sen on määritelty RFC 2917-dokumentissa. Tiivistettyä todentamisesta käytetään päätepisteen todentamisessa, sitä voidaan käyttää myös käyttäjien todentamisessa välityspalvelimille, välityspalvelimien käyttäjille sekä tietoliikennepakettien todennusotsikkokentissä. (Understanding Voice over IP Security 2006, 147-151).

Pretty good privacy (PGP) määritellään RFC 2543-dokumentissa, jossa myös alkuperäinen SIP-protokolla määritellään. PGP:tä käytetään SIP-yksityisyyden, -todentamisen ja -yhtenäisyyden varmistamiseen.

Alkujaan PGP kehitettiin Phil Zimmermanın toimesta sähköpostiviestien suojaamiseen.

Secure/Multipurpose Internet Mail Extension (S/MIME) tarjoaa keinon suojata SIP viestien eheyttä sekä luottamuksellisuutta. Päätepiste voi digitaalisesti allekirjoittaa koko viestin tai osan siitä. Digitaalisen allekirjoituksen avulla voidaan määrittämää onko viestiä muutettu matkalla.

S/MIME:ä voidaan käyttää SIP-protokollassa seuraavin tavoin:

1. Viestin sisällön salakirjoitukseen, koko viestin sisältö voidaan salakirjoittaa.
2. Koko SIP-viestin yksityisyyden ja eheyden suojaamiseen. Koko SIP-viesti tai vastaus voidaan salakirjoittaa ja toimittaa viestin sisältönä. Vastaanotettaessa sisältö puretaan ja verrataan vastaanotettuun SIP-viestiin.

(Understanding Voice over IP Security 2006, 153-155).

SIP pystyy hyödyntämään siirtokerroksen suojausta, Transport Layer Security (TLS), hyppy hypyltä-periaatteella suojaamaan signaalintiviestejä päätepiisteeltä välityspalvelimelle tai call servereille.

TLS:n kättely etenee täsmälleen samalla tavoin kuin suojatuissa verkkotapahtumissakin. Välityspalvelin tarjoaa digitaalisen varmenteen ja päätepiiste yrittää varmentaa palvelimen seuraavanlaisesti:

1. Ettei varmenne ole vanhentunut.
2. Että varmenteen myöntäjä on päätepiisteiden hyväksymä.
3. Että subjectAltName kattaa koko etäosoitteen.
 - a. Jos päätepiiste lähettää pyynnön, niin subjectAltName-kentän tulee vastata osoitetta, johon pyyntö lähetettiin.
 - b. Jos päätepiiste vastaanotti pyynnön, niin subjectAltName-kentän tulee vastata osoitetta ylemmässä Via-otsikkokentässä.
4. Että vastapuolen IP-osoite löytyy DNS:ä käyttäen.

(Understanding Voice over IP Security 2006, 155-159).

Suojattu SIP on Uniform Resource locator (URI) pohjainen sips -viesti, jota käytetään pyydetäessä, että TLS suojaa jokaisen hypyn signaaloinnin aikana. Soittajalta soitettavan domainiin asti. (Understanding Voice over IP Security 2006, 159-160).

2.8.6 Secure RTP

VoIP-media siirretään käyttäen RTP-protokollaa. RTP Control-protokolla (RTCP) toimittaa tieto ja hieman hallintaa RTP-istuntoihin. RTCP:n kontrollointi rajoittuu pääasiallisesti ryhmä- ja monilähetysistuntoihin. Pisteestä pisteeseen tapahtuvassa mediaistunnossa, kuten VoIP, RTCP:tä käytetään puheenlaaturaporttien vaihtamiseen.

SIP voi avata useita samanaikaisia mediaistuntoja, audio- tai videoliikennettä. Jokainen RTP-liikenne tapahtuu eri UDP-portista ja sillä on oma yksilöllinen synchronization source (SSRC) -tunniste.

Secure RTP on profiililaajennus RTP:n, joka lisää luotettavuuden, todennuksen ja eheyden suojausta RTP-istuntoihin. SRTP lisää RTP-liikenteeseen salakirjoituksen ja eheyden suojauksen ennen kun mediaistunto luovutetaan UDP:lle siirrettäväksi.

SRTP käyttää symmetrisiä avaimia ja koodeja medialiikenteen salakirjoitukseen, muttei tarjoa avainten hallintaa tai yleistä toiminnallisuutta. (Understanding Voice over IP Security 2006, 164-168).

2.8.7 PSTN-yhdyskäytävän suojaus

VoIP-laitteiden ja PSTN-verkon välille tarvitaan yhdyskäytäviä, jotta liikenne saadaan reititettyä verkosta toiseen.

PSTN verkossa suojaus on enemmän toteutettu fyysisesti eristämällä verkko kuin salakirjoittamalla tai koodaamalla liikenne. Signaaloinnin peukalointia vastaan PSTN-verkossa käytetään eri signaalointiprotokollia luotetuille ja ei-luotetuille elementeille. PSTN-verkoilla on myös suojaus palveluhyökkäyksiä vastaan, sekä tahallisia että tahattomia. (Understanding Voice over IP Security 2006, 225-227).

Vaikka PSTN -yhdyskäytävä on pääasiassa SIP VoIP-arkkitehtuurissa päätepiste (tai useita päätepisteitä), niin sen toiminnassa on joitain yksilöllisiä näkökohtia:

1. PSTN-yhdyskäytävän käyttö puhekäytössä voi aikaansaada huomattavaa kulutusta ja käsikäsipääsyhyökkäyksiä.
2. PSTN-yhdyskäytävät voivat toimia hyökkäyskohtina PSTN puhelinkytkeisiin tai Signaling System#7 (SS7) verkkoihin.
3. Soittolinjan tunnisteen, calling line ID (CLID), ja muiden PSTN tunnistetietojen käyttö on tarkoin säänneltyä. Monissa hallintoalueissa CLID:tä väärinkäyttävä PSTN-yhdyskäytäväoperaattori voidaan tuomita sakkoihin tai rangaistustuomioihin.
4. Puhelinhakkeroijat saattavat yrittää hyödyntää yhdyskäytäviä PSTN:n puolelta hyökätäkseen VoIP-verkkoon.

(Understanding Voice over IP Security 2006, 227-228).

2.8.8 Yhdyskäytävän turva-arkkitehtuuri

Useat VoIP-päätelaitteiden turvallisuusperiaatteet vaikuttavat yleisesti PSTN-yhdyskäytäviin. PSTN-yhdyskäytävät eivät yleensä toimi itsenäisinä osina vaan niiden ja päätelaitteiden välissä on yleensä välityspalvelin, samoin PSTN-yhdyskäytävä ei todenna myöskään VoIP -käyttäjiä. SIP-välityspalvelin ja PSTN-yhdyskäytävä ovat osa samaa toimialuetta ja ylläpitävät suojattua signaalintisuhdetta, joka havaitsee ja hylkää viestit, jotka yrittävät ohittaa suojausvälityspalvelimen.

Yhdyskäytävää ylläpitävän operaattorin tulee voida todentaa käyttäjät, jotta laskutus voidaan ohjata oikealle käyttäjälle. Useimmilla PSTN operaattoreilla on kehittynyt, reaaliaikainen petostenhavainnointijärjestelmä, joka monitoroi puheluiden yksityiskohtaraportteja sekä raportoi poikkeavuuksista.

2.8.9 Yhdyskäytävätyypit

VoIP yhdyskäytäviä on kahdenlaisia, perustuen protokollaan, jolla ne avaavat yhteyden PSTN:n.

Teleliikenteentarjoajat pitävät yritysytteyskäytäviä ulkoisina verkkoelementteinä, ne eivät toimi teleliikenteentarjoajan toimialueella, eikä PSTN:n luottamusta laajenneta niihin. Tämän vuoksi yritysytteyskäytävät muodostavat yhteyden PSTN:N käyttäen User to Network Interface (UNI)-protokollia.

Verkkoyhdyskäytävää sen sijaan pidetään luotettuna elementtinä. Sitä pidetään oleellisesti osana PSTN-kytkinverkkoa ja se muodostaa yhteyden käyttäen Network to Network Interface (NNI) -protokollia. Vahvistaminen ja henkilöllistietojen tarkastus tapahtuvat verkon yhdyskäytävän toimesta. (Understanding Voice over IP Security 2006, 229-230).

2.8.10 Yhdyskäytävät ja soittajatunniste

PSTN-verkossa henkilöllisyys osoitetaan loppukäyttäjille soittaja tunnisteena (caller ID) tai soittavan linjan tunnisteena (calling line ID, CLID). Caller ID on PSTN:lle tärkeä palvelu, sitä käytetään tarkastukseen, kirjaamiseen ja muihin palveluihin. Caller ID:tä ei käytetä kuitenkaan laskutukseen.

Maaailmanlaajuisessa PSTN-puhelinverkossa caller ID tunniste vakuutukset turvautuvat siirtävään luottamukseen. Luotettavan verkkoelementin vakuuttama tunniste on luotettava myös muiden PSTN:n verkkoelementtien mielestä, huolimatta siitä mikä lähde tunniste on luotettavaksi määritellyt. (Understanding Voice over IP Security 2006, 230-231).

2.8.11 Soittajatunniste ja yksityisyys

Useissa paikoissa PSTN-soittajat voivat estää soittajatunnisteensa näkymisen. Kuitenkin PSTN:ssä estetty soittajatunniste on muiden toimialueen puhelinkytkeinten saatavilla. Tämä tieto kuljetetaan NNI-liityntöjen yli, mutta poistetaan ennen kuljettamista UNI-liityntöjen yli, eli kun poistutaan toimialueen ulkopuolelle.

Jos verkkokytkin vastaanottaa tällaista tunnistetietoa NNI-liitynnästä, niin sen ei tarvitse välittää sitä UNI-liitäntäisille VoIP-verkon elementeille.

Tyypillisesti PSTN yhdyskäytävä on kuitenkin osa toimialuetta. (Understanding Voice over IP Security 2006, 231).

2.8.12 Yhdyskäytävän dekomponointi

Jos yhdyskäytävä dekomponoidaan käyttäen master/slave dekomponointiprotokollia, niin protokollien tarpeellisia turvamekanismeja tulee käyttää, esimerkiksi IP Securitya (IPSec) mediayhdyskäytävän (MG) ja mediayhdyskäytäväkontrollerin (MGC) välillä. (Understanding Voice over IP Security 2006, 231).

2.8.13 SIP/ISUP-välinen toiminta

PSTN-yhdyskäytävien signaalitoiminto silttaa IP-pohjaisen ja PSTN-verkon. Yhdyskäytävät käyttävät yksityiskohtaista kartoittamista kahden äänisignaalin välillä suoriutuakseen siitä. Esimerkiksi SIP-liikenne PSTN-yhdyskäytävälle noudattaa SIP/ISUP kuvausmäärittelyä, ja H.323 ja PSTN:n välinen toiminta tapahtuu, kuten se on määritelty H.246:ssa.

Yhdyskäytävät on testattava, jotta varmistetaan, etteivät epätavalliset, epämuotoiset tai kelvottomat SIP-viestit leviä PSTN-verkkoon.

ISUP-tunnelointi PSTN-verkkojen välillä tarkoittaa sitä, että PSTN toimialuetta laajennetaan IP-verkon yli. Käytännössä tämä tapahtuu siten, että PSTN-soittaja soittaa PSTN-verkosta IP-verkon kautta toiseen PSTN-verkkoon. PSTN-verkossa media kulkee ISUP-muodossa ja IP-verkossa SIP-muodossa.

Tällöin on käytettävä vahvimpia turvatoimenpiteitä, kuten:

1. Yhdyskäytävien vahva päästä päähän ja hypyltä hypylle todentaminen.
2. Salakirjoittaminen tietosuojan vuoksi.
3. Eheyden suojaaminen.

ISUP-tunneloinnin toteuttaminen ilman näitä suojaustoimenpiteitä heikentää PSTN-ympäristön suojausta. (Understanding Voice over IP Security 2006, 232-233).

2.8.14 Puhelinnumeroiden kartoittaminen DNS:ssä

Electronic Number Mapping System (ENUM) hyödyntää DNS:ä kartoittaakseen PSTN puhelinnumeron Internet-osoitteeksi. ENUM lupaa auttaa yhdistämään VoIP-liitettävyyden ”saarekkeet” yhtenäiseksi. Esimerkiksi nykyään soittaessa VoIP-palveluntarjoajan verkosta toiseen VoIP-palveluntarjoajan verkkoon, reitittyy puhelu PSTN-verkon kautta. ENUM:ia käytettäessä se VoIP-palveluntarjoaja, jonka verkosta puhelu alkaa, tekee DNS-kyselyn käyttäen valittua puhelinnumeroa, selvittää että puhelinnumero kuuluu VoIP-päätelaitteelle ja reitittää puhelun Internet-verkossa.

Vaikkakin ENUM tarjoaa välineet edellä mainitun toteuttamiseen, on palveluntarjoajien silti oltava valmiita vaihtamaan VoIP-liikennettä toistensa kanssa.

(Understanding Voice over IP Security 2006, 233-236).

2.8.15 VoIP ja hätäpuhelut

Soittaessa VoIP-liittymästä hätänumeroon voi ilmentyä ongelmia, jos soittajalla on käytössään VPN-yhteyteen sidottu kiinteä IP-osoite. Tällöin puhelu ei välttämättä reitity lähimpään hätäkeskukseen käyttäjän sijainnin mukaan vaan IP-osoitteen sijainnin perusteella.

3 VOIP-JÄRJESTELMÄT

Tässä luvussa avataan VoIP-järjestelmiä. Luvussa selvitetään, mistä eri komponenteista, laitteista ja ohjelmistoista VoIP-järjestelmä muodostuu sekä miten ne liittyvät toisiinsa. Luvussa käsitellään myös eri tiedonsiirtoprotokollia sekä sitä, miten ne nivoutuvat yhteen. Luvussa esitellään myös, miten mobiili- ja analogilaitteet liitetään osaksi VoIP-järjestelmää.

3.1 VoIP-järjestelmien laitteistokokoonpano

3.1.1 Kuluttajasovellukset (järjestelmät)

Internet-operaattoreiden tarjoamissa VoIP-palveluissa loppukäyttäjä voi siirtää nykyisen lankanumeronsa tai tilata uuden numeron oman alueensa suuntanumerolla. Puheluita voidaan soittaa SIP-protokollaa tukevilla VoIP-puhelimilla, lankapuhelimilla tiettyjen modeemien kautta, tietokoneen kautta (erillisellä usb-puhelimella tai kuulokkeet ja mikrofonin) tai useilla Nokian multimediapuhelimilla. (Saunalahti Group Oyj 2008).

Vertaispalveluista Windows Messenger ja Skype toimivat tietokoneelle asennettavana soveluksena. Niiden käyttö vaatii tietokoneeseen liitetyn kuulokkeet ja mikrofonin tai USB-liitännäisen puhelimen. (Windows Live Messenger 2008, Skype 2008).

3.1.2 Yrityskäyttöön soveltuvat järjestelmät

Tässä luvussa avataan pääpiirteittäin yrityskäyttöön soveltuvien järjestelmien kokoonpano. Tässä mainittujen elementtien lisäksi tarvitaan muut toimivat TCP/IP-verkon komponentit.

3.1.2.1 Päätelaitteet

Päätelaitteina voidaan käyttää SIP-protokollaa tukevia VoIP-puhelimia, lankapuhelimia VoIP-sovittimien kanssa, matkapuhelimia Voice over Wireless LAN- (VoWLAN) tukiasemien kanssa. SIP-protokollaa tukevia VoIP-puhelimia valmistaa esimerkiksi Cisco Systems Inc. (Cisco Systems Inc. 2009)



Kuva 7: Cisco IP Puhelin 7960G. (Cisco 2009)

Tietokoneelle asennettavien sovellusten, esimerkiksi SAP Business Communications Management Softwaren kanssa voidaan käyttää USB-liitäntäisiä kuulokkeita ja mikrofoneja tai puhelimia. (SAP Global 2009).

3.1.2.2 PSTN-yhdyskäytävät

PSTN-yhdyskäytävä mahdollistaa puheluiden reitittämisen PSTN-verkon ja tietoverkon välillä, yhdyskäytävä muuntaa televiestinnän IP-protokollaksi. (3CX Ltd 2009).



Kuva 8: Cisco AS5350 Universal Gateway. (Cisco 2009)

3.1.2.3 Yhdyskäytävät

Yhdyskäytävät yhdistävät eri hallinnollisissa toimialueissa sijaitsevat VoIP-verkot toisiinsa. Yhdyskäytävät ovat verkon reunalla sijaitsevia reitittämiä tai reitittäviä palomureja. (Cisco Systems Inc. 2009)

Yhdyskäytävä on laite, joka pystyy yhdistämään eri protokollia käyttäviä verkkoja toisiinsa. Yhdyskäytävän pitää olla sekä reititin että siihen yhdistyneen erilaista verkkoprotokollaa käyttävän verkon vastaava laite. (TCP/IP-verkot 2002, 31).

3.1.2.4 Reitittimet

Reititin hallitsee IP-tason protokollat, eli reitittää IP-paketit kohti oikeaa kohdeverkkoa. (TCP/IP-verkot 2002, 31).

3.1.2.5 Palomuurit ja reitittävät palomuurit

Palomuri sijaitsee yleensä yrityksen sisäverkon ja julkisen verkon rajalla, kuitenkin sisäverkon puolella. Palomuurilla voidaan myös rajata erilaisia sisäverkon osia tai kaikille avoimia vierailijaverkkoja. Palomuri estää asiattoman pääsyn lähiverkon osiin. Palomuurilla voidaan myös rajoittaa ulospäin suuntautuvaa liikennettä. Vähimmäisvaatimus palomuurille on sen kyky analysoida vähintään IP-kerroksen paketteja. Tehokkaammat palomuurit pystyvät analysoimaan myös muiden protokollakerrosten tietoja.

Palomuri voi toimia myös reitittimenä, sekä reititin palomuurina. Kuitenkin jos kuormitus kasvaa, on kannattavaa eriyttää laitteet ja niiden toiminnot, jolloin eri laitteet hoitavat reititys- ja suodatustoiminnot. (TCP/IP-verkot 2002, 32).

3.1.2.6 Palvelimet

VoIP-järjestelmään kuuluu olennaisena osana palvelin tai palvelimet, jotka huolehtivat verkossa tapahtuvista puheluista. Alla mainittavat toiminnot voivat olla eriytettyinä omille palvelimilleen tai integroituna samaan palvelimeen.

SIP-palvelin hoitaa kaikki verkossa tapahtuvat SIP-puhelut, sitä voidaan myös kutsua rekisteröijäksi tai SIP-välityspalvelimeksi. (3CX Ltd 2009).

STUN-palvelin (Simple Traversal of User Datagram Protocol Through Network Address Translators) mahdollistaa sen, että NAT-laitteen asiakkaat voivat luoda paikallisen verkon ulkopuolella olevaan VoIP-palvelimeen. STUN-palvelimella asiakkaat saavat tietoonsa julkisen osoitteen, NAT-laitteen tyyppin ja Internetin puoleisen portin, jonka NAT-laite on liittänyt paikalliseen porttiin. Näiden tietojen avulla on mahdollista luoda UDP-yhteys asiakkaan ja VoIP-palvelimen välillä, jotta puhelu voidaan luoda. (3CX Ltd 2009, IETF 2009).

Cisco Unified Communications Manager (CallManager) on kaiken kattava VoIP-järjestelmä. Siihen kuuluvat palvelimet ja ohjelmistot, joita tarvitaan VoIP-järjestelmän toimintaan. Call-

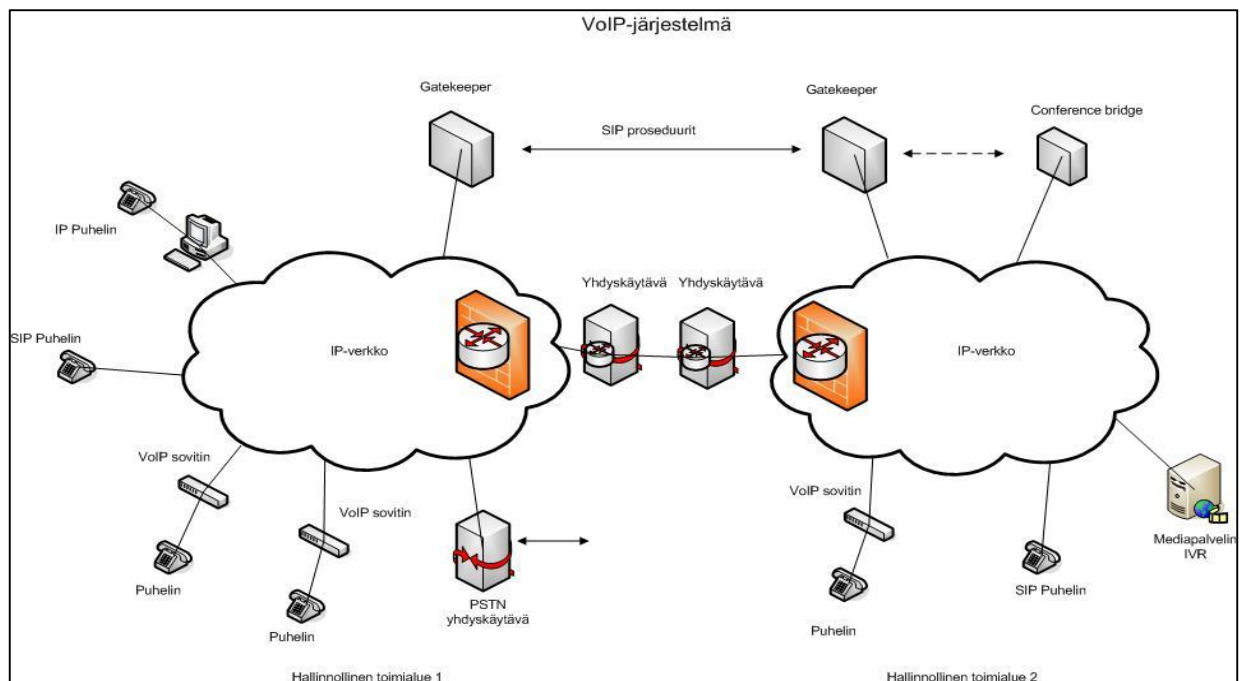
Manageriin voidaan liittää ja rekisteröidä puhelimia, yhdyskäytäviä, gatekeepereitä sekä mediaressursseja. Mediaressursseja ovat esimerkiksi Conference Bridget (CFB), joita tarvitaan neuvottelupuheluiden luomiseen ja ylläpitoon. (Cisco Systems Inc. 2009).

3.1.2.7 Ohjelmistot

Ohjelmistoihin kuuluvat työasema- ja palvelinohjelmistot sekä sovellukset.

Työasemasovellukset ovat yleensä VoIP-järjestelmän hallintasovelluksia, VoIP-sovelluksia puhelin- ja osoitekirjatoiminnoilla tai vaihde- ja jononhallintatoiminnoilla. (SAP Global 2009).

Palvelinohjelmistoihin kuuluvat: puhelunkäsittely ja -valvontasovellukset. Kokoonpanotietokannat, joissa on laitteiden kokoonpanotiedot. Puhelinjärjestelmän hallintasovellukset. Analysointi- ja raportointisovellukset, joilla saadaan yksityiskohtaisia tietoja puheluista ja niiden laadusta. Conference Bridge (CFB) -sovellukset sekä osoitekirjan synkronointisovellukset, joilla voidaan synkronoida Microsoft Outlook ja Outlook Express osoitekirjat VoIP-järjestelmän osoitekirjan kanssa. (Cisco Systems Inc. 2009).



Kuva 9: VoIP-järjestelmän kuvaus. (Muokattu Douskalis 2002)

3.2 Mobiililaitteiden liittäminen VoIP-järjestelmään

Yritykset hyödyntävät VoWLAN sovelluksia saadakseen tarjotakseen työntekijöilleen mahdollisuuden mobiliteettiin sekä karsiakseen tavallisen verkkoinfrastruktuurin aiheuttamia kustannuksia. Useissa tapauksissa VoWLAN toteutetaan langallisen VoIP-järjestelmän laajenuksena. Langattomia VoIP-järjestelmiä löytyy nykyään suuryrityksistä, yliopistoista ja muista oppilaitoksista, varastorakennuksista, tuotantolaitoksista, pienyrityksistä ja kodeista. (Wireless-Nets, Ltd 2008).

VoIP-järjestelmään liitettävät mobiililaitteet voivat olla joko matkapuhelimia, joissa on WLAN-sovitin tai langattomia VoIP-puhelimia. Mobiililaite voi olla myös kannettavalla tietokoneella käytettävä VoIP-sovellus, jota käytetään WLAN-verkon yli. (Cuuma Communications 2009).

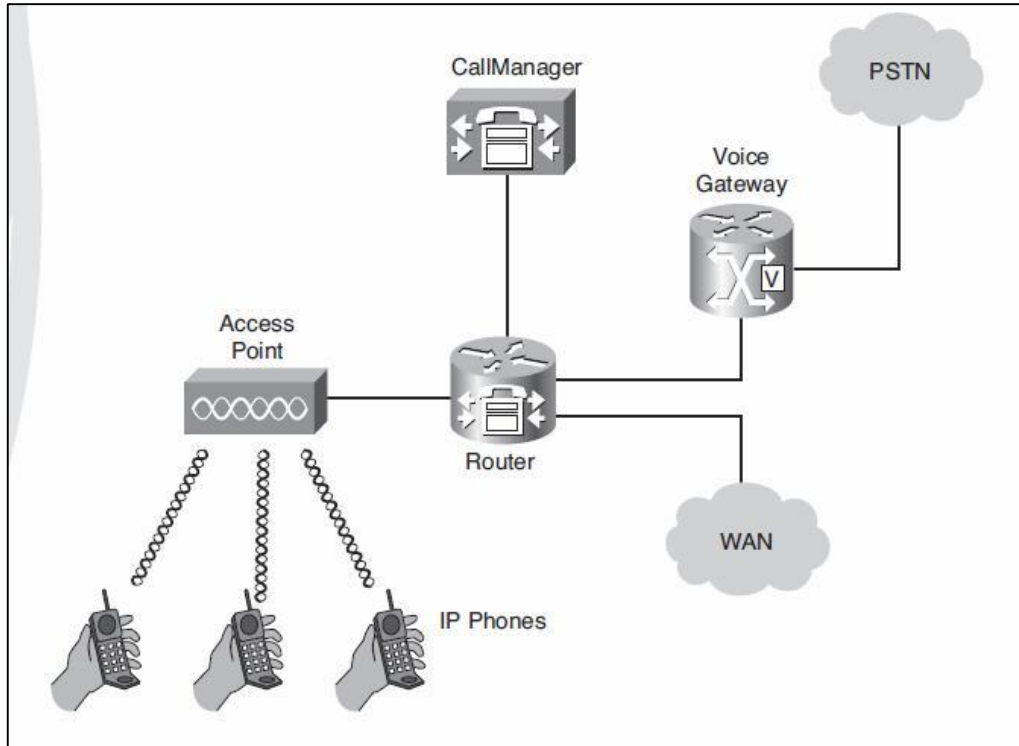
VoWLAN-järjestelmään tarvitaan vähintään seuraavat komponentit:

1. Langaton IP-puhelin
WLAN-sovittimen sisältävä matka- tai VoIP-puhelin.
2. Call Manager
Call Manager käsittelee verkon puhelut sekä suorittaa toimintoja, kuten IP puhelinten rekisteröinnin, soitto- ja reitityskarttojen hallinnoinnin sekä vastaajien hallinnan.
3. Ääniyhdyskäytävä, PSTN-yhdyskäytävä
4. WLAN-infrastruktuuri
Langaton LAN-verkko huolehtii langattomien VoIP-puheluiden kuljettamisesta toimipaikassa.

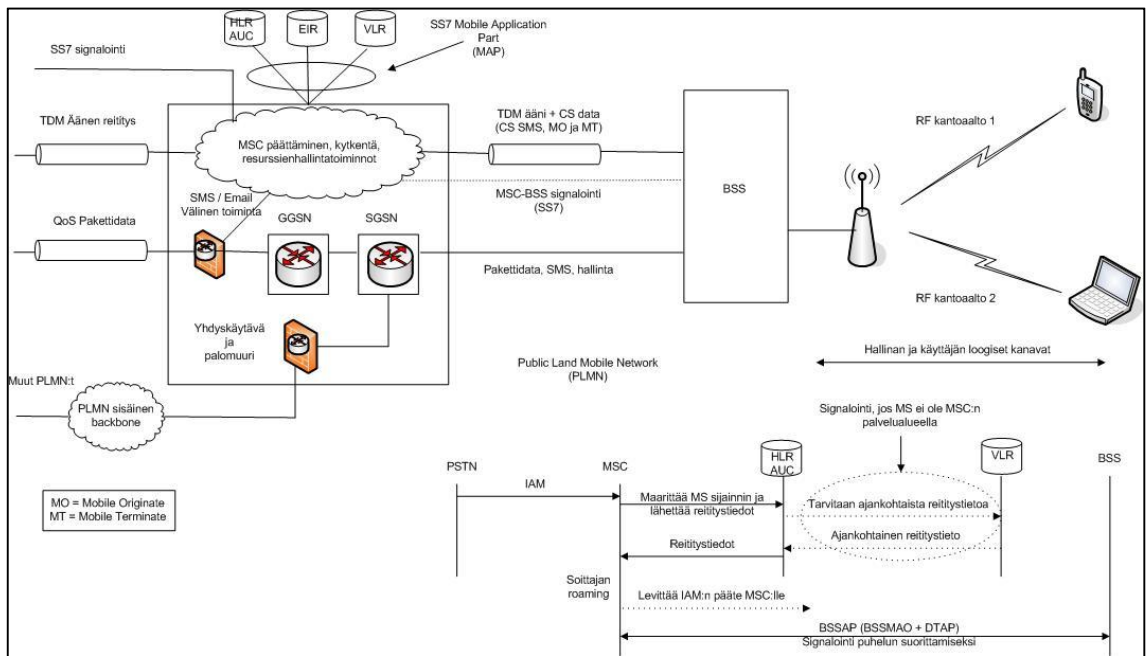
Jotta käyttäjien langattomat IP-puhelimet toimisivat, täytyy puhelimen WLAN-sovittimen yhdistyä tukiasemaan. Kun puhelu aloitetaan, pyyntö kulkee tukiasemasta langattoman verkon kautta Call Managerille, joka käsittelee pyynnön. Jotta saataisiin liikkuvuutta, WLAN-sovitin yhdistyy muihin tukiasemiin tarpeen mukaan. Puhelu ei katkea, jos siirtyminen tukiasemalta toiselle kestää alle 100 millisekuntia. Jos viive on suurempi, katkeaa puhelu yleensä.

Soitettaessa ulkoiseen numeroon Call Manager ohjaa puhelun PSTN-yhdyskäytävälle tai Internetiin.

Esimerkiksi Microsoft Windows -pohjaista Cisco IP Softphone -sovellusta voidaan käyttää fyysisen päätelaitteen sijaan. Sovellus asennetaan kannettavalle tietokoneelle, jossa on WLAN-sovitin, ja käytetään joko USB-liitäntäistä puhelinta tai kuulokkeita ja mikrofonia. (Wireless-Nets, Ltd 2008).



Kuva 10: Ensijaiset VoWLAN järjestelmän komponentit. (Wireless-Nets, Ltd 2008)



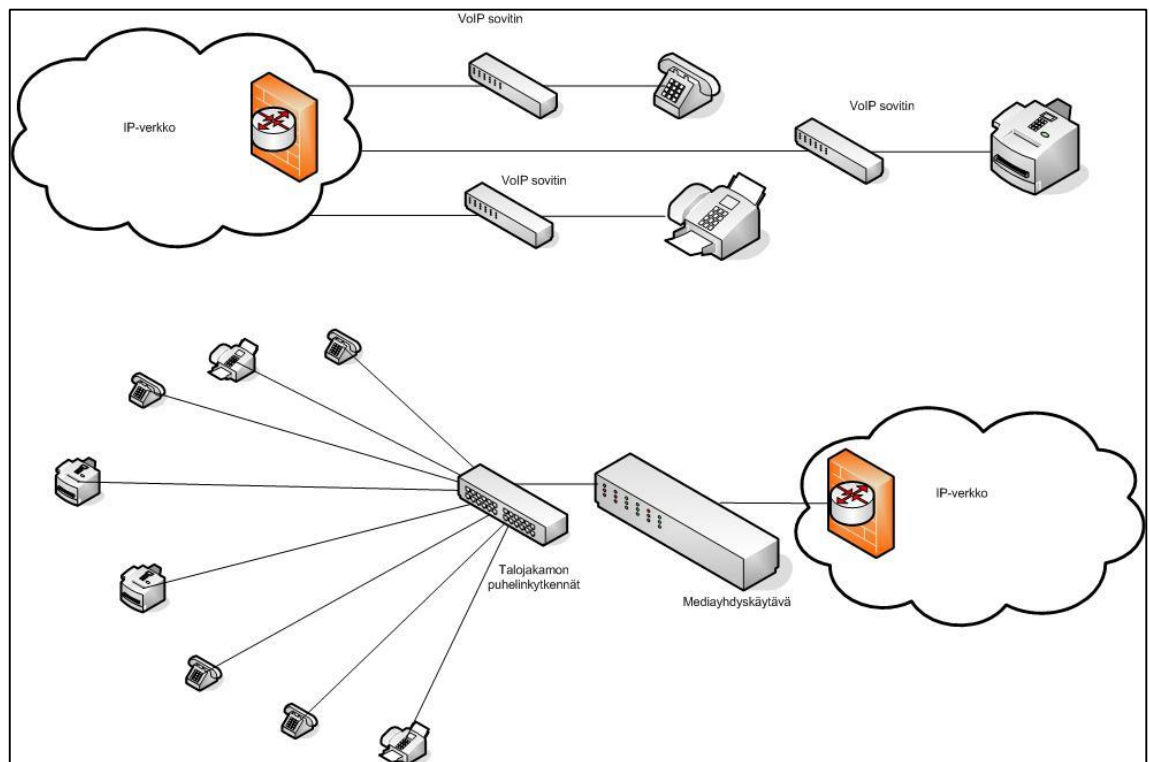
Kuva 11: Mobiililaitteiden liittäminen VoIP-järjestelmään. (Muokattu Douskalis 2002)

3.3 Analogilaitteiden liittäminen VoIP-järjestelmään

Tässä opinnäytetyössä analogilaitteilla tarkoitetaan perinteisen puhelinjärjestelmän laitteita, lankapuhelimia, fakseja, monitoimilaitteita eli laitteita, jotka tukevat muita kuin SIP- ja H.323-protokollia.

Perinteisen puhelinjärjestelmän laitteet tukevat G.729, G.729A, G.729AB2, G.723.1, G711a-law ja G.711 μ -law äänikoodekkeja sekä G.711 ja T.38 faksikoodekkeja. (Cisco Systems Inc 2009).

Näiden laitteiden VoIP-järjestelmään liittämiseen tarvitaan sovittimia, VoIP-sovittimia tai mediayhdyskäytäviä, jotka kykenevät muuntamaan laitteiden lähettämän koodekin VoIP-järjestelmissä käytettyihin koodekkeihin.



Kuva 12: Analogilaitteiden liittäminen VoIP-järjestelmään.

3.3.1 Yksittäisten analogilaitteiden liittäminen (VoIP-sovitin)

Yksittäisten laitteiden liittämisessä voidaan käyttää VoIP-sovitinta, joista esimerkkinä Cisco ATA 186 (Analog Telephone Adapter).



Kuva 13: Cisco ATA 186 VoIP-sovitin. (Cisco 2009)

Cisco ATA 186 muuntaa perinteisen puhelinjärjestelmän laitteen IP-laitteeksi. Sovitin tukee kahta ääniporttia, joihin saadaan itsenäinen puhelinnumero sekä yhtä 10BaseT Ethernet-porttia. VoIP-sovitin kytketään LAN-verkkoon RJ-45 ethernet kaapelilla ja puhelinlaitteet sovittimeen RJ-11 kaapeleilla.

Cisco ATA 186 tukee H.323 v2 ja v4, SIP, MGCP1.0 sekä SCCP VoIP-protokollia.

Tuetut faksiprotokollat ovat G.711 μ -law sekä G.711 A-law. Tästä aiheutuu se, ettei Cisco ATA 186 pysty toimimaan G3 faksien ja monitoimilaitteiden kanssa, sillä se tukee maksimissaan nopeuksia 14.4 kbps, kun nopeimmat laitteet pystyvät 33.6 kbps nopeuteen. (Cisco Systems Inc 2009).

3.3.2 Useiden analogilaitteiden liittäminen (Mediayhdyskäytävä)

Useiden laitteiden liittämisessä saman toimipaikan VoIP-järjestelmään voidaan käyttää mediayhdyskäytävää, kuten AudioCodes MediaPack 100-sarjan tuotteita.



Kuva 14: Audiocodes MediaPack 100-sarjan Mediayhdyskäytäviä. (Audiocodes 2009)

Mediayhdyskäytävässä on mallista riippuen 2 - 24 analogista porttia, ja se tukee perinteisen puhelinjärjestelmän laitteita tai analogisia runkojohtoja. AudioCodesin tuotteet ovat myös T.38 yhteensopivia, joten ne tukevat nopeampaa faksiliikennettä sekä G3 laitteita. Tuettuja VoIP-protokollia ovat MGCP, H.323(V4) sekä SIP. AudioCodes Mediayhdyskäytävä kytketään talojakamon LSA-riipaan, kiinteistön puhelininfrastruktuuriin ja IP-verkon väliin. (AudioCodes Limited 2003 -2009).

4 TOTEUTUS

4.1 Vanha infrastruktuuri ja sen hyödyntäminen

Vanhaa IT-infrastruktuuria pyritään hyödyntämään VoIP-järjestelmän toteutuksessa mahdollisimman paljon. Tämä edellyttää verkon komponenteilta yhteensopivuutta VoIP-järjestelmän kanssa. Mahdollisesti epäsovivat komponentit tulee korvata sopivilla laitteilla, ennen kuin siirtymisen toteutus on mahdollinen.

4.2 Fyysinen järjestelmä

VoIP-järjestelmä toteutetaan käyttäen Fujitsun konesalissa sijaitsevia, asiakkaan omia tai Fujitsulta vuokrattuja palvelimia. Konesaliratkaisun toteutuksessa käytetään Cisco Media Convergence Series 7800 -sarjan palvelimia tai hyväksytyjä kolmannen osapuolen palvelimia. Cisco Media Convergence Series 7800 -sarjan palvelimia ovat Cisco MCS 7816, MCS 7825, MCS 7828, MCS 7835 ja MCS 7845. Hyväksytyjä kolmansien osapuolien palvelimia valmistavat HP ja IBM. Palvelimille asennetaan Cisco Unified Communications Manager Version 7.1 (Call-Manager), kaikkine ohjelmistoineen. Järjestelmä itsessään on fyysisesti hajautettu ja kahdennettu sekä infrastruktuuriltaan että tietoliikenteeltään. Käytettävyys toteutetaan keskitetyllä prosessien hallinnalla ja prosessien tilatiedon seurannalla. Kuntayhtymän ympäristöt tulevat sijaitsemaan kahdessa eri fyysisessä sekä loogisessa installaatiossa. Mahdollisten käyttöhäiriöiden sattuessa palvelu siirtyy näiden välillä ilman katkoksia.

Fujitsu toimii kuntayhtymän operaattorina, puhelut reititetään Fujitsun konesalissa sijaitsevien järjestelmien kautta kuntayhtymän IP-verkkoon, jossa kuntayhtymän omat puhelunvälittäjät tarvittaessa ohjaavat puhelut eteenpäin.

Kuntayhtymän IT-infrastruktuurissa tulee olla VoWLAN käyttöön sopivat WLAN-tukiasemat, jotta Nokia E-sarjan matkapuhelimia voidaan käyttää VoIP-käytössä.

4.3 Käyttöliittymät ja päätelaitteet

VoIP-järjestelmä toteutetaan kuntayhtymän toiveen mukaan ns. yhden puhelimen käytön mukaan. Kiinteissä toimipisteissä työskenteleville käyttäjille tarjotaan joko Cisco VoIP-toiminnepuhelinta tai SAP-mobiilivaihteen Microsoft Internet Explorer (IE) pohjaista käyttöliittymää. Cisco VoIP-toiminnepuhelin tarjotaan erityisryhmille, jotka tarvitsevat johtaja-sihteeri ominaisuuksia tai vastaajaryhmiä. Liikkuville työryhmille ja käyttäjille tarjotaan Nokia E-sarjan matkapuhelinta, jota voidaan käyttää joko matkapuhelinverkossa tai toimipisteiden VoWLAN-verkoissa.

Liittymävaihtoehdot ovat matkapuhelinliittymä, työasemapuhelin, työasemapuhelin ja matkapuhelinliittymä ja laaja matkapuhelinliittymä.

Mobiilivaihteen käyttöliittymä on selainpohjainen (IE), jolloin ei tarvita paikallisia asennuksia työasemiin. Asiakkaan käyttöliittymässä on puhelunhallintatyökalut; soittaminen, puheluiden kääntö, poiminta, yhdistäminen, siirto ja neuvottelu.

Käyttöliittymässä on kommunikaatio- ja hakemisto-osa. Kommunikaatio-osaan sisältyy viestipalvelut kun hakemisto-osa toimii osoitekirjan tavoin. Viestipalvelut sisältävät puhelut, tekstiviestit, pikasanomat ja kuntayhtymän sisäiset chat-yhteydet.

4.4 Puhelunvälitys

Puhelunvälitys toteutetaan kuntayhtymän omalla puhelunvälityshenkilöstöllä. Puhelunvälityksessä käytetään Fujitsun toimittamaa mobiilivaihtepalvelua, joka koostuu siihen liitetyistä matka- ja lankaverkon kutsunumeroista. Välitystoiminta tapahtuu mobiilivaihteen Puhelunvälittäjä-toiminnoilla. Perinteinen puhelinverkon vaihde voidaan siirtymän ajaksi liittää mobiilivaihteeseen.

Voidaan tehty keskitetysti tai hajautetusti toimipaikkoihin

Kullekin käyttäjälle on yksi julkinen, joko matka- tai lankaverkon, kutsunumero. Puheluiden välitystoiminta tapahtuu mobiilivaihteen Puhelunvälittäjä-toiminnoilla. Perinteinen puhelinverkon vaihde voidaan liittää mobiilivaihteeseen (siirtymävaiheen ajaksi). Puhelunvälittäjillä on käytössään selainpohjainen (IE) käyttöliittymä, jolloin vaihteenhoitaja voi työskennellä miltä tahansa kuntayhtymän IT-verkkoon kytketyltä työasemalta. Tämä mahdollistaa sen, että vaihteenhoitaja voi työskennellä myös pienistä toimipisteistä tai etäyhteydellä, sekä vaihteenhoidon keskittämisen tai hajauttamisen useisiin toimipisteisiin.

4.5 Mobiililaitteiden liittäminen VoIP-järjestelmään

Mobiililaitteiden liittämistä varten kuntayhtymän IT-infrastruktuurin täytyy olla ajantasainen. Käytettävien WLAN-tukiasemien tulee mielellään olla malliltaan Cisco Aironet sarjan tukiasemia tai muita, jotka mahdollistavat mobiililaitteen siirtymisen tukiasemalta toiselle alle sadan millisekunnin.

Järjestelmään liitettävät mobiililaitteet tulevat olemaan Nokian E-sarjan matkapuhelimia.

4.6 Analogilaitteiden liittäminen VoIP-järjestelmään

Analogilaitteiden liittämisessä hyödynnetään olemassa olevia perinteisen puhelinjärjestelmän kaapelointeja.

Suuremmissa toimipisteissä faksien, monitoimilaitteiden ja perinteisen puhelinjärjestelmän neuvottelupuhelinten liittämiseen käytetään AudioCodes MediaPack MP-124D yhdyskäytävää, joka liitetään talojakamossa olemassa olevaan verkkoon sekä Fujitsun verkkoon. Pienemmissä toimipisteissä sekä yksittäisten laitteiden liittämässä käytetään Cisco ATA 186 -sovittimia.

5 HANKKEEN ARVIOINTI

Opinnäytetyön arvioinnissa on hyödynnetty Janne Laaksosen ja hänen ryhmänsä tekemää arviota. Janne Laaksonen toimii ryhmäesimiehenä Fujitsu Services Oy:llä.

Opinnäytetyön lähtökohdan valinnassa on onnistuttu hyvin, sillä kuntayhtymän tarjouspyyntö on monimuotoisuudessaan hyvä esimerkki puhepalveluympäristöstä, jonka toteutus tuo esiin VoIP-tekniikan mahdollistamat hyödyt. Lähtökohtaan liittyvät myös käyttöönoton tuomat haasteet. Tekijä on sisäistänyt hyvin opinnäytetyön lähtökohtana olleen kuntayhtymän tarjouspyynnön, sen nykytilakuvauksen sekä asiakkaan tavoitteet tulevan järjestelmän osalta.

VoIP-tekniikan ja -palveluiden perustiedot on käyty läpi tasolla, joka palvelee opinnäytetyön kohderyhmää, Fujitsu Services Oy:n myynti- ja projektihenkilöstöä. Opinnäytetyö mahdollistaa sen tietojen hyödyntämisen tarjottavan ratkaisun suunnittelussa.

Opinnäytetyössä on käsitelty poikkeuksellisen kattavasti VoIP-järjestelmiin liittyviä tietoturvaa ja siihen liittyviä riskejä. Tämä on Fujitsun kannalta positiivinen asia, mutta riskien osalta opinnäytetyössä olisi voinut olla ratkaisuja niiden poistoon tai minimointiin. Kuitenkin kyseinen osio on hyödynnettävissä myynti- ja projektihenkilöstön lisäksi myös asiantuntijatasolla.

Laitteisto ja palveluympäristöt on käsitelty VoIP-järjestelmäosassa riittävällä tarkkuudella, ja niiden pääpaino on Ciscon järjestelmissä. Esimerkkijärjestelmät vastaavat hyvin Fujitsun järjestelmätarjoumaa. Esimerkkejä on mahdollista hyödyntää tarjoussuunnittelussa ja ympäristömäärityksessä.

Puutteita opinnäytetyössä ovat hieman suppeasti kuvatut hyödyt, joita VoIP-järjestelmät tuovat koko asiakkuudelle sekä yksittäiselle ala-liittymäkäyttäjälle. Fujitsu olisi jäänyt kaipaamaan perusteluita, joilla asiakas saadaan tekemään päätös siirtymään käyttämään VoIP-palveluympäristöä.

Kokonaisuutena opinnäytetyö täyttää sille asetetut tavoitteet, ja se on hyödynnettävissä etenkin tarjouspyyntövaiheen ympäristömäärityksessä. (Opinnäytetyön arviointi 2009)

Kirjoittajan mielestä opinnäytetyön aihepiiri oli laaja, ja kyseisestä viitekehystä olisi saanut kirjoitettua useamman yksityiskohtaisen raportin tai opinnäytetyön. Kyseinen opinnäytetyö on tarkoitettu Fujitsu Services Oy:n myynti- ja projektihenkilöstön käyttöön, VoIP-materiaaliksi. Opinnäytetyön tarkoituksena on tukea ja antaa tarvittavaa tietoa Fujitsun henkilöstölle VoIP-projekteihin. Tekijän mielestä tässä tehtävässä on onnistuttu.

Lähteet

- 3CX Ltd 2009. Software Based PBX for Windows. [www-sivu].
<<http://www.3cx.fi/voip-sip/voip-gateway.php>>. (Haettu 11.10.2009).
- AudioCodes Limited 2003-2009. SIP MediaPack Installation Guide version 5.6. [pdf-dokumentti].
<<http://www.audiocodes.com/downloads/>> (Haettu 27.6.2009).
- Baron, D. 2005. SIP Basics. Massachusetts Institute of Technology [ppt-esitys].
<<http://www.internet2.edu/sip.edu/200507-workshop/NP133.PPT>>
(Haettu 27.6.2009).
- Bateman, D. 2005. Configuring CallManager and Unity: A Step-by-Step Guide. Neljäs painos. USA, Indianapolis: Cisco Press.
- Chappel, L. 1999. Cisco reitittimet. Suomentaja Jani Ilkka. Jyväskylä: Gummerus Kirjapaino Oy.
- Cisco Systems 2009. Cisco ATA 186 Analog Telephone Adapter. [www-sivu].
<http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps514/ps515/product_data_sheet09186a008007cd72.html> (Haettu 27.10.2009).
- Cisco Systems Inc 2009. Routers. [www-sivu].
<<http://www.cisco.com/en/US/products/hw/routers/index.html>>.
(Haettu 10.10.2009).
- Cisco Systems Inc 2009. Voice and Unified Communications. [www-sivu].
<<http://www.cisco.com/en/US/products/sw/voicesw/index.html>>.
(Haettu 10.10.2009).
- Cuuma Communications 2009. VoIP-päätelaitteet. [www-sivu].
< <http://www.cuuma.com/?sivu=2&sub=24> > (Haettu 26.10.2009).
- Douskalis, B. 2002. Putting VoIP to Work. USA, New Jersey: Prentice-Hall PTR.
- Fujitsu Services Oy. 2009. Opinnäytetyön arviointi.
- Fujitsu Services Oy. 2007. Puhepalvelut, palvelukuvaus.
- Johnston, A & Piscitello, D. 2006. Understanding Voice over IP Security. USA, Massachusetts: Artech House, INC.
- Kaario, K. 2002. TCP/IP-verkot. Porvoo: WS Bookwell.
- Liikenne- ja viestintäministeriö. 2005. Internet-puhelut (VoIP) selvitys. Helsinki: Edita Prima Oy.
- Microsoft Corp. 2008. Windows Live Messenger. [www-sivu].
<<http://get.live.com/messenger/overview>>. (Haettu 1.3.2008).
- SAP Global 2009. SAP Business Communications Management. [www-sivu].
< <http://www.sap.com/solutions/business-suite/crm/businesscommunications/featuresfunctions/index.epx>>.
(Haettu 3.10.2009).
- Saunalahti Group Oyj 2008. Saunalahti Nettipuhelin. [www-sivu].
<<http://saunalahti.fi/nettipuhelin/>>. (Haettu 1.3.2008).

Skype Limited 2008. [www-sivu].
<<http://www.skype.com/intl/fi>>. (Haettu 1.3.2008).
The Internet Engineering Task Force (IETF) 2009. STUN- Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). [www-sivu].
<<http://www.ietf.org/rfc/rfc3489.txt>>. (Haettu 11.10.2009).

Welho Tietoa Welhosta 2008. [www-sivu].
<<http://www.welho.fi/Yksityisille/TietoaWelhosta/tabid/163/Default.aspx>>. (Haettu 1.2.2008).

Wireless-Nets, Ltd 2008. Chapter 2, CoWLAN System Components [pdf-dokumentti].
<http://www.wireless-nets.com/resources/downloads/VoWLAN_C2.pdf>
(Haettu 24.10.2009).

XXX seudun kuntayhtymä. 2007. Xxx seudun puhetietoliikenteen kokonaispalvelun tarjouspyyntö.

Kuvat

Kuva 1: Asiakkaan nykytila. (Muokattu Xxx seudun kuntayhtymä 2007)	9
Kuva 2: Asiakkaan tavoitetila. (Muokattu Xxx seudun kuntayhtymä 2007)	11
Kuva 3: OSI- ja TCP/IP -mallin kuvaus. (Muokattu Kaario 2002).....	17
Kuva 4: Puhelun muodostaminen H.323 protokollaa käyttäen. (Muokattu Douskalis 2002)	19
Kuva 5: Puhelun muodostaminen SIP protokollaa käyttäen (Proxy). (Muokattu Douskalis 2002)	21
Kuva 6: Puhelun muodostaminen SIP protokollaa käyttäen (Gateway). (Muokattu Douskalis 2002)	23
Kuva 7: Cisco IP Puhelin 7960G. (Cisco 2009).....	35
Kuva 8: Cisco AS5350 Universal Gateway. (Cisco 2009)	35
Kuva 9: VoIP-järjestelmän kuvaus. (Muokattu Douskalis 2002).....	37
Kuva 10: Ensisijaiset VoWLAN järjestelmän komponentit. (Wireless-Nets, Ltd 2008).....	39
Kuva 11: Mobiililaitteiden liittäminen VoIP-järjestelmään. (Muokattu Douskalis 2002).....	39
Kuva 12: Analogilaitteiden liittäminen VoIP-järjestelmään.	40
Kuva 13: Cisco ATA 186 VoIP-sovitin. (Cisco 2009).....	41
Kuva 14: Audiocodes MediaPack 100-sarjan Mediayhdyskäytäviä. (Audiocodes 2009).....	41