TEKNIIKKA JA LIIKENNE

Tietotekniikka

Tietoverkot

INSINÖÖRITYÖ

VOIP-JÄRJESTELMIEN INTEGROIMINEN

Työn tekijä: Tero-Pekka Pajunen
Työn ohjaaja: Marko Uusitalo

Työ hyväksytty: ___. ___. 2011

Marko Uusitalo
lehtori

ALKULAUSE

Tämä projekti tehtiin Metropolia Ammattikorkeakoululle. Käytännön työvaiheet toteutettiin koulun laboratorioluokassa. Kiitän saamastani aiheesta ja neuvoista työn ohjaajaa lehtori Marko Uusitaloa. Lisäksi haluan antaa erityiskiitokset vaimolleni Emmi Pajuselle saamastani kannustuksesta.

Helsingissä 11.7.2011

Tero-Pekka Pajunen

Metropolia

TIIVISTELMÄ

Työn tekijä: Tero-Pekka Pajunen	
Työn nimi: VOIP-järjestelmien integroiminen	
Päivämäärä: 11.7.2011	**Sivumäärä:** 59 s. + 1 liitettä
Koulutusohjelma: Tietotekniikka	**Suuntautumisvaihtoehto:** Tietoverkot
Työn ohjaaja: lehtori Marko Uusitalo	

Tämä insinöörityö tehtiin Metropolia Ammattikorkeakoululle. Työssä tutkittiin koulun laboratorioluokan VoIP-puhelinjärjestelmiä ja tehtiin niihin jatkoasennuksia. Tavoitteena oli yhdistää erilliset järjestelmät yhdeksi kokonaisuudeksi, jossa puheliikenne kulkisi saumattomasti eri VoIP-palvelinten välillä. Lisäksi järjestelmään asennettiin laajennus, joka mahdollisti puheliikenteen GSM- ja IP-verkon välillä.

Työn teoriaosassa esitellään SIP-signalintiprotokollaa käyttävän VoIP-verkon kannalta keskeisiä asioita, kuten äänen digitointia, VoIP-liikenteen muita protokollia, ominaisuuksia ja tietoturvaa. Lisäksi esitellään työssä käytetyt laitteet, kuten Portech MV-372 -GSM-VoIP-yhdyskäytävä, Cisco Call Manager- ja Trixbox- VoIP-palvelimet ja Cisco 7960 -IP-puhelin sekä niiden hallintaan käytetyt yhteysprotokollat, kuten HTTPS, SSH ja Telnet.

Työ alkoi GSM-VoIP-yhdyskäytävän asentamisella järjestelmään. Tarvittaviin asetuksiin perehdyttiin ja laite konfiguroitiin reitittämään puhelut GSM-verkon ja IP-verkon välillä. Trixbox-VoIP-palvelin konfiguroitiin yhdyskäytävästä tulevien puheluiden aktiiviseksi puhepalvelimeksi sekä kaikkien GSM-verkkoon soitettavien puheluiden kauttakulkukeskukseksi. Trixboxin lisäksi toisina VoIP-palvelimina toimivat Cisco Call Manager ja Cisco Unified Communications 520. Jokaiseen VoIP-palvelimeen rekisteröitiin laboratoriossa vähintään yksi pöytäpuhelin, minkä lisäksi kokeiltiin tietokoneeseen asennetun ohjelmistopuhelin X-Liten toimintaa internetin yli.

Tässä työssä VoIP-puheluiden signalointiprotokollaksi valittiin SIP-protokolla, jonka toimintaan sekä laitekohtaiseen konfigurointiin perehdyttiin pääasiassa internetistä löydettyjen ohjeiden avulla. Myös monien muiden laiteasetusten säätämiseen ja ominaisuuksien käyttöönottoon löytyi tukea alan foorumeiden avulla. Lopputuloksena syntyi toimiva integraatio, jossa puhelut kulkivat sujuvasti eri palvelimiin rekisteröityjen puhelinten välillä sekä GSM- ja VoIP-verkon välillä. Äänenlaatu todettiin hyväksi kaikissa puheluissa, eikä internetin tai gsm-verkon huomattu heikentävän puheen laatua.

Avainsanat: VoIP, SIP, puhelinvaihde, IP-puhe, gsm-voip-yhdyskäytävä

Metropolia

ABSTRACT

Name: Tero-Pekka Pajunen

Title: Intergrating VoIP systems

Date: 11 July 2011 **Number of pages:** 59 + 1 appendix

Department: Information Technology

Study Programme: Data Networks

Instructor: Marko Uusitalo, Senior Lecturer

This final project was made for Metropolia University of Applied Sciences. This work studies the school laboratory class VoIP phone systems, to which follow-up installations were conducted in this project. The aim was to combine separate systems into a single entity, where voice traffic would seamlessly traverse different VoIP servers. In addition, an extension was installed to the system, which allowed the transport of voice between GSM and IP network.

The theoretical part presents the VoIP network using SIP signaling protocol in terms of key issues, such as the digitization of audio, VoIP traffic, other protocols, features, and information security. It also presents the work equipment used, such as Portech MV-372 VoIP GSM Gateway, Cisco Call Manager and Trixbox VoIP servers and Cisco 7960 IP phone. The most essential connection protocols such as HTTPS, SSH and Telnet are also presented.

The work was started by installing the GSM VoIP gateway to the system. The settings were studied and the device was configured to route calls between GSM network and an IP network. Trixbox VoIP server was configured as an active call server for incoming calls from GSM gateway, as well as a transit center for all the calls directed to GSM network. In addition to Trixbox, the other VoIP servers run on Cisco Call Manager and Cisco Unified 520. Each of the VoIP servers was registered with at least one desktop phone in the laboratory. In addition, the X-Lite software phone operation over the internet was experimented.

In this work, the SIP protocol was selected as the signaling protocol for VoIP calls. Its operation principles were studied and device specific configurations examined with the help of guides and instructions that were mainly found from the Internet. Many other device settings were set and features were learned with the support provided by different forums of industry. The end result was a functional integration of VoIP systems, where calls smoothly traversed the servers between phones, and between GSM and VoIP network. Sound quality was found equally good in calls in laboratory environment, in calls through internet, and in calls utilizing the GSM network.

Keywords: VoIP, SIP, network, IP phone, gsm voip gateway

SISÄLLYS

KÄSITTEET JA LYHENTEET

ARP	Address Resolution protocol. Protokolla, joka selvittää IP-osoitteita vastaavat laitekohtaiset MAC-osoitteet.
DHCP	Domain Host Configuration Protocol. IP-osoitteiden dynaamiseen jakamiseen käytetty protokolla.
DNS	Domain Name System. Internetin nimipalvelujärjestelmä.
DSP	Digital Signal Processor. Digitaalinen signaaliprosessori analogisten ja digitaalisten signaalien sovittamiseen keskenään.
GNU	GNU's Not Unix. Projekti, jonka tavoitteena on kehittää täysin vapaa käyttöjärjestelmä.
HTTP	Hyper Text Transfer Protocol. Asiakaskoneen internetselaimen ja palvelimen välillä toimiva yhteysprotokolla.
IETF	Internet Engineering Task Force. Internet-protokollien standardoinnista vastaava organisaatio.
IP	Internet Protocol. Hoitaa pakettien toimittamisen oikeaan osoitteeseen pakettikytkentäisessä verkossa.
ITU-T	Internetional Telecommunication Union-Telecommunication Stadardization Sector. Kansainvälisen televiestintäliiton telestandardointisektori.
LAN	Local Area Network. Lähiverkko.
OSI	Open Systems Interconnection. Tietoliikennejärjestelmien välisen tiedonkulun suunnitteluun käytetty malli.
PBX	Private Branch Exchange. Yksityinen puhelinvaihde.
PCM	Pulse Code Modulating. Menetelmä, jolla signaali koodataan digitaaliseen muotoon.
PoE	Power over Ethernet. Standardoitu tekniikka, joka mahdollistaa sähkön siirron verkkokaapelin välityksellä.
QoS	Quality of Service. Tietoliikenteen luokittelun ja priorisoinnin kattotermi.
RTP	Real Time Protocol. Reaaliaikaisen tiedon siirtoon IP-verkoissa käytetty protokolla.
SIP	Session Initiation Protocol. VoIP-puheluissa käytetty merkinantoprotokolla.
TCP	Transport Control Protocol. IP-pakettien perillemenon varmistava yhteydellinen OSI-mallin kuljetuskerroksen protokolla IP-pakettien siirtoon

TLS	Transport Layer Security. I-liikenteen salausprotokolla, joka kehitettiin SSLv3:sta.
UDP	User Datagram Protocol. Yhteydetön ja epäluotettava kuljetuskerroksen protokolla IP-pakettien siirtoon.
VAD	Voice Activity Detection. Puheen aktiivisuuden tunnistukseen puheen prosessoinnissa käytetty tekniikka.
VoIP	Voice over IP. IP-puheluiden siirtämiseen dataverkossa käytetty tekniikka.
WAN	Wide Area Network. Laajaverkko.
IS	Integrated Services. Verkon kapasiteetin ennalta varaamiseen käytetty palvelu.

1 JOHDANTO

Työn tarkoituksena oli jatkokehittää koulun VoIP-puhelinjärjestelmää paremmin skaalautuvaksi kokonaisuudeksi ja liittää siihen uusia ominaisuuksia. Työn teoriaosassa esitetään järjestelmän keskeiset elementit ja niiden toiminta sekä toiminnan kannalta oleelliset protokollat. Koska työ toteutettiin käyttämällä SIP-merkinantoprotokollaa, ei vanhempaa H.323-protokollaa esitellä tässä työssä. Sen lisäksi tarkastellaan muita järjestelmän luotettavan ja turvallisen toiminnan kannalta tärkeitä asioita, jotka on hyvä huomioida jo järjestelmän suunnitteluvaiheessa.

Työ jakautuu integraation osalta kolmeen vaiheeseen, joissa tarkastellaan kahta toisiinsa liitettävää järjestelmää tai niiden osaa. Integraatiolla tarkoitetaan tässä työssä järjestelmien yhteenliittämistä. Ensimmäinen työvaihe sisältää GSM-VoIP-yhdyskäytävän asentamisen, minkä jälkeen VoIP-puhelinjärjestelmä voi kommunikoida matkapuhelinverkon kanssa. Työn toisessa vaiheessa sovitettiin yhteen kaksi valmiiksi asennettua VoIP-järjestelmän palvelinyksikköä: Cisco Call Manager sekä Trixbox. Työssä esitellään palvelinten perustiedot sekä käydään läpi ne asetukset, joita ominaisuuksien ja palvelinten välisen kommunikaation käyttö edellyttää. Viimeisessä työvaiheessa integraatioon liitettiin Cisco Unified 520 -VoIP-palvelinyksikkö, jossa on myös analogisia FXS-portteja sekä digitaalisia BRI-portteja. Kiinteiden koulussa sijaitsevien puhelinten lisäksi asennettiin vielä yksi X-Lite-ohjelmistopuhelin, jolla puheyhteyttä pystyttiin kokeilemaan kauempaa koulun sisäverkon ulkopuolelta.

Kaikkien työvaiheiden onnistumisen tuloksena syntyi kolmen VoIP-järjestelmän integraatio, jossa puheluiden laatu todettiin kaikissa testeissä hyväksi. Tulos kuvastaa VoIP-järjestelmien toimivuutta ja hyvää skaalautuvuutta, sekä eri laite- ja ohjelmistovalmistajien tuotteiden helppoa integroitumista yhdeksi toimivaksi kokonaisuudeksi. Järjestelmää on mahdollista jatkokehittää tulevaisuudessa ja liittää siihen uusia ominaisuuksia, kuten videopuheluita tukevia laitteita.

2 VOIP

VoIP-käsitteen avulla kuvataan reaaliaikaista äänen ja videokuvan siirtämistä IP-verkossa. Tässä luvussa käydään läpi digitaalisen median peruspiirteet sekä Voice Over Internet Protocol -tekniikan toiminta laitteiston, protokollien ja verkon kapasiteetin osalta SIP-protokollaa käytettäessä.

2.1 Digitaalisuus

Analogisen signaalin hyvin tunnettu heikkous on sen kuljettaminen pitkiä matkoja. Signaaliin syntyy häiriöitä, jotka voimistuvat, kun signaalia vahvistetaan sen heikkenemisen vuoksi. Lopulta signaalin häiriöt ovat niin suuria, että signaalin hyöty menetetään. Digitaalitekniikka esittelee uuden ja häiriösietoisemman tavan siirtää signaalia sähköisesti. Signaalia voidaan vahvistaa vahvistamatta häiriöitä. Myös vahvistamattoman signaalin kantomatka on pidempi. Useissa tapauksissa tiedon kulku verkon yli digitaalisessa muodossa on osittaista, eikä esimerkiksi puhelu välttämättä kulje aivan päästä päähän digitaalisesti.

2.1.1 Digitointi

Digitaalisuudessa asiat esitetään diskreetein, täsmällisin arvoin, joita on rajallinen määrä, kun taas analoginen tieto tallennetaan portaattomalla asteikolla. Yleensä digitaalinen data esitetään binäärimuodossa eli ykkösinä ja nollina.

Muunnos analogisen ja digitaalisen tiedonesitystavan välillä voidaan toteuttaa esimerkiksi tehtävään dedikoidun digitaalisen signaaliprosessorin, DSP:n (Digital Signal Prosessor) avulla, mutta myös tavallinen nykyaikainen yleiskäyttöprosessori voidaan valjastaa tehtävään ohjelmallisesti. Nykyisillä prosessoreilla riittää laskentatehoa AD/DA -muunnoksiin muiden tehtävien ohella, eikä käskykannan tarvitse olla kyseiseen tehtävään optimoitu. AD (Analog to Digital) -muunnos on prosessi, jossa analoginen signaali koodataan digitaaliseksi ja DA-muunnoksessa digitaalinen signaali muunnetaan takaisin analogiseksi.

Aaltomuotokoodekkeihin kuuluva, digitaalisissa puhelinverkoissa käytettävä, PCM (Pulse Code Modulating) -koodaus toteuttaa AD-muunnoksen nelivaiheisesti suodatuksen, näytteistyksen, kvantisoinnin ja koodauksen avulla.

Suodatuksessa päästetään läpi vain halutuntaajuiset signaalit, jolloin osa virheistä häviää. Normaalien puhetaajuuksien vaihdellessa välillä 200-2800 Hz on puhetta äänittävien laitteiden suunnittelussa päädytty tavallisesti 4000 Hz:n taajuuskaistaan. Näytteistyksessä signaalista otetaan näytteitä (jännitearvoja) tietyllä taajuudella, joka on puheen näytteistyksessä perinteisesti 8000 Hz. Nyquistin mukaan näytteistyksessä käytetyn taajuuden on oltava vähintään kaksinkertainen signaalin korkeimpaan taajuuteen verrattuna, jotta digitaalinen ääninäyte saataisiin jälleen muutettua takaisin analogiseen muotoon. Kvantisoinnissa näytteet pyöristetään lähimpään ennalta määritellyn arvoasteikon arvoon, joita esimerkiksi puhekäyttöön soveltuvassa G.711-standardin PCM-koodauksessa on 256 kappaletta ja joista kukin edustaa kahdeksanbittistä binäärilukua. Kvantisoinnissa tehtävät pyöristykset aiheuttavat virheitä, jotka ilmenevät nk. kvantisointikohinana. [1.]

Kvantisoinnin yhteydessä suoritetaan myös kompandointi (eng. companding = compressing+expanding), mikä tekee arvoasteikosta logaritmisen. Signaali pakataan lähetyspäässä ja puretaan alkuperäiseen kokoonsa vastaanottopäässä. Kompandoinnissa näytteitä otetaan sitä tiheämmin mitä matalampi äänenvoimakkuus on. Tällä korostetaan pienten äänenvoimakkuuksien välisiä eroja, jolloin suhteellinen tarkkuus eri äänenvoimakkuuksilla pysyy yhtenäisempänä. Kompendoinnista on olemassa kaksi vaihtoehtoista menetelmää: A-laki ja U-laki (u-law ja a-law). U-laki on käytössä Pohjois-Amerikassa ja Japanissa, kun taas A-laki kattaa pääosin Euroopan ja muut alueet. Myös kansainväliset yhteydet käyttävät A-laki-standardia. Lopuksi näytteet koodataan siirtoa tai tallennusta varten sopivampaan muotoon. [1; 2, s. 27.]

2.1.2 Puhekoodekit

Puhekoodekit ohjaavat signaalin muuntamista, pakkaamista ja purkamista. Pakkaamaton puhesignaali vie enemmän kaistaa kuin pakattu. Esimerkiksi 8 kHz:n näytteenottotaajuudella ja 8 bitin PCM-koodauksella digitoitu puhe vie kaistaa 64 kbps (8 bit * 8 kHz), mikä on yleisen televerkon puhekaistan perusyksikkö. PCM-koodauksesta on myös kehitetty muunneltuja versioita, jotka vievät vähemmän kaistaa. DPCM (Differential PCM) kvantisoi vain signaalien välisiä pieniä eroja pystyen täten vähentämään näytteisiin tarvittavien bittien määrää. ADPCM (Adaptive DPCM) esittelee signaalin vaihtelun ennustettavuuden, jonka avulla kvantisointitasojen esitystarkkuutta voidaan säätää tilanteen mukaan [1].

PCM-menetelmän lisäksi ääntä voidaan pakata myös puhetta mallintamalla, jolloin päästään hyvin alhaisiin bittinopeuksiin. LPC (Linear Predictive Coding) on mallintamisessa paljon käytetty menetelmä, jolla puheen voi pakata jopa alle 2 kbps:n kaistalle, mutta tällöin myös puheen laatu kärsii huomattavasti. Hybridikoodekki pyrkii hyödyntämään edellä mainittujen hyvät puolet, jotta bittinopeus pysyisi alhaisena ja äänenlaatu säilyttäisi luonnollisuutensa. Hybridimenetelmiä ovat mm. CELP (Codebook Excited Linear Prediction), LD (Low-Delay) -CELP, CSA (Conjugate Structure Algebraic) -CELP, MP-MLQ (Multi-Pulse, Multi-Level Quantization) ja ACELP (Algebraic Code Excited Linear Prediction). Taulukossa 1 on vertailtu eräitä ITU-T:n standardoimia äänenpakkauskoodekkeja. [2.]

Taulukko 1. Puhekoodekit [2, osa 3, s. 32]

Koodekki		Bittinopeus (kbps)	MIPS	Näytteen koko (ms)	MOS
G.711	PCM	64	0,34	0,125	4,1
G.726	ADPCM	32	13	0,125	3,85
G.728	LD-CELP	13	33	0,625	3,61
G.729	CSA-CELP	8	20	10	3,92
G.729a	CSA-CELP	8	10,5	10	3,9
G.723.1	MPMLQ	6,3	16	30	3,9
G.723.1	ACELP	5,3	16	30	3,8

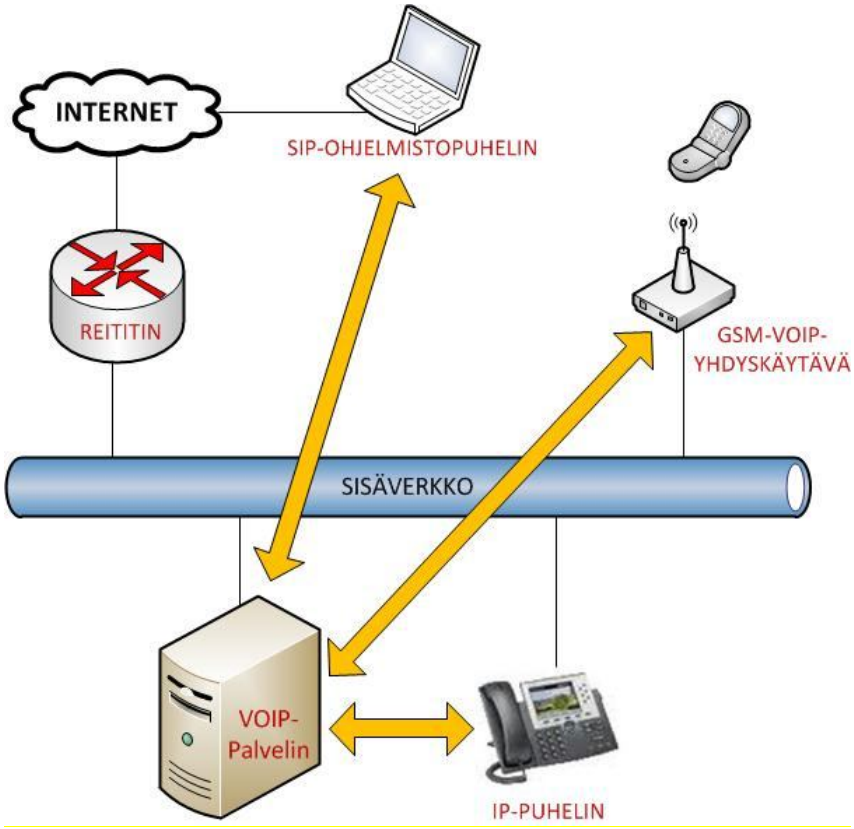
Taulukosta huomataan, miten tehokkaampi pakkaus vaikuttaa bittinopeuteen, laskutehovaatimukseen (Million Instruction per second, MIPS) ja äänen laatuun (Mean Opinion Score , MOS) sekä minkä kokoisia näytteitä eri koodekit käyttävät. Kuten taulukosta nähdään, vaatii tehokkaampi koodaus keskimäärin myös enemmän laskentatehoa monivaiheisempien laskutoimitusten suorittamiseen. Äänen laadun arvioiminen MOS-asteikolla perustuu testei-

hin, joissa koehenkilöt arvioivat ääninäytteen laatua asteikolla yhdestä viiteen [3, s. 5]. Näytteen koko (ms) kertoo, kuinka pitkän pätkän signaalia yksi näyte sisältää. Esimerkiksi PCM-koodattu puhe 8 kHz:n näytteenottotaajuudella ottaa näytteen 8000 kertaa sekunnissa, jolloin näytteen pituudeksi tulee 0,000125 sekuntia.

2.2 IP-PBX-puhelinjärjestelmä

Perinteisellä PBX-järjestelmällä tarkoitetaan yleensä yrityksen tai yhteisön omaa, yksityistä järjestelmää puheluiden ohjausta varten. Puhelinvaihteen englanninkielinen vastine, Private Branch eXchange(PBX), kuvaa hyvin sen yksityistä luonnetta. Puhelinvaihdetta käytetään perinteisesti puheluiden yhdistämiseen. Pääasiassa tämä koskee sisäverkon puheluita, mutta vaihteesta on yleensä myös yhteys runkolinkin kautta operaattorin keskukseen televerkossa tai dataverkossa. Runkolinkki mahdollistaa monta samanaikaista yhteyttä saman linkin kautta. Ilman puhelinvaihdetta jokainen puhelin, jopa samassa rakennuksessa, jouduttaisiin kytkemään erikseen operaattorin verkkoon. Tämän seurauksena myös yrityksen sisäiset puhelut olisivat maksullisia, koska ne kiertäisivät julkisen televerkon kautta. Yksityisen puhelinvaihteen ansiosta sisäverkon puhelut eivät aiheuta kustannuksia ja nykyaikaisten VoIP-vaihteiden ominaisuuksiin myös monia muita hyödyllisiä palveluita, jotka olivat kalliita toteuttaa perinteisellä PBX-järjestelmällä.

IP-PBX -järjestelmä, toiselta nimeltään VoIP-järjestelmä, on modernimpi versio, joka käyttää vanhan puhelinverkon sijaan IP-verkkoja puheluiden ja multimedian kuljettamiseen. IP-PBX-palvelin eli VoIP-palvelin sisältää useimmiten monia hienoja ominaisuuksia, joita on helppo toteuttaa ja ottaa käyttöön erilaisten ohjelmistojen avulla. Puheluiden ohjaus, joka on useimmiten VoIP-palvelimen olennaisin toiminto, toimii täysin ohjelmallisesti. Palvelin sisältää tietokannan muun muassa siihen rekisteröidyistä puhelimista ja muista järjestelmän laitteista ja voi nopeasti kytkeä puheluita niiden välillä. Kuva 1 esittää VoIP-puhelinjärjestelmää, jossa on palvelimen lisäksi kolme erilaista päätelaitetta: tavallinen IP-puhelin, ohjelmistopuhelin ja GSM-VoIP-yhdyskäytävä.



Kuva 1. VoIP-puhelinjärjestelmä.

2.3 SIP-signalointiprotokolla

Session Initiation Protocol on IETF:n standardoima (RFC 3261-3265) merkinantoprotokolla, jota käytetään IP-verkossa muodostamaan, ylläpitämään ja purkamaan istuntoja kahden tai useamman päätelaitteen välillä. Istunnot voivat sisältää yhtä tai useampaa mediaa, kuten ääntä ja videokuvaa. SIP tukee myös monia muita palveluita, kuten pikaviestintää, saatavuuspalvelua, tiedostojen siirtämistä, pelaamista ja ohjelmien jakamista.

2.3.1 SIP-verkon komponentit

SIP-verkon rakenne perustuu asiakas-palvelin-malliin, jossa asiakas lähettää pyyntöjä, joihin palvelin vastaa. SIP-verkon komponentteja ovat käyttäjäagentit (User Agent, UA) ja palvelimet. Käyttäjäagentit ovat sovelluksia, jotka hoitavat istuntokohtaisen kommunikoinnin käyttäjän puolesta. Käyttäjäagentti voi toimia yhdessä kahdesta roolista:

- Asiakasosa (User Agent Client, UAC) aloittaa SIP-pyynnön.
- Palvelinosa (User Agent Server, UAS) käsittelee pyynnön, muodostaa yhteyden käyttäjään ja palauttaa vastauksen käyttäjän puolesta.

SIP-verkon fyysiset laitteet voidaan lajitella asiakkaisiin ja palvelimiin. SIP-asiakkaita ovat:

- Puhelin: Voi toimia joko UAC:n tai UAS:n roolissa, eli kykenee luomaan ja käsittelemään pyyntöjä.
- Yhdyskäytävä: Sovittaa liikenteen erityyppisten verkkojen ja päätelaitteiden välillä, esimerkiksi GSM-verkosta IP-verkkoon tai perinteisen puhelinverkon ja ip-verkon välillä. Sisältää kuljetusmuotojen ja kommunikointimenetelmien välisen käännöstyön lisäksi puheluiden muodostamisen ja lopettamisen molempien verkkojen kanssa sekä audio- ja videokoodekkien muunnokset.

SIP-palvelimia ovat:

- Välityspalvelin: Välittää SIP-pyyntöjä aina eteenpäin seuraavalle palvelimelle. Pyynnöt voivat kulkea usean palvelimen kautta ennen saapumistaan päämääräänsä. Välityspalvelimien tarjoamia muita ominaisuuksia ovat autentikointi, autorisointi, pääsynhallinta (Network Access Control, NAC), reititys, luotettava pyynnön uudelleenlähetys ja turvallisuus.
- Uudelleenohjauspalvelin: Ei luo eikä välitä pyyntöjä, vaan kertoo asiakassovellukselle uuden osoitteen, johon pyyntö pitäisi lähettää.
- Rekisteröintipalvelin: Rekisteröi käyttäjät ja ylläpitää listaa asiakkaiden IP- ja SIP-osoitteista. Välittää tiedon paikannuspalvelimelle pyynnön jälkeen.

Palvelimet voivat sijaita erillään tai fyysisesti samassa paikassa. Rekisteröintipalvelin sijaitsee usein välityspalvelimen yhteydessä [2, osa 3, s. 2, 3; 5, s. 2, 3; 4, s. 63].

2.3.2 SIP-protokollan toiminta

SIP käyttää ASCII-koodia, joten se on http:n ja smtp:n tavoin tekstipohjainen protokolla. Jokainen SIP-verkon asiakas, joka muodostaa tai vastaanottaa puheluita, erotellaan uniikin SIP-osoitteen avulla. Osoitteet ovat sähköpostiosoitteen kaltaisia ja ovat muotoa: SIP:userID@domain.com.

SIP-protokollan toiminta perustuu seuraaviin viiteen toiminteeseen:

- Käyttäjän sijainti: selvittää istuntoon osallistuvan päätelaitteen sijainnin verkossa.
- Käyttäjän ominaisuudet: määrittelee päätelaitteen tukemat median-siirto-ominaisuudet.
- Käyttäjän käytettävyys: selvittää, voidaanko istunto päätelaitteeseen muodostaa.
- Puhelun muodostus: muodostaa yhteyden ja valitsee yhteyden parametrit päätelaitteiden välille
- Puhelun hallinta: määrittelee puhelun ylläpitoon ja lopetukseen vaadittavat toimenpiteet.

SIP osaa tulkita sekä verkkotunnuksia että IP-osoitteita ja kykenee päätelaitteiden välisen liikenteen uudelleenohjaukseen. Uudelleenohjaus mahdollistaa varsinaisen liikenteen siirtymisen käyttämään uutta reittiä. Istunnon kuvaukseen eli istunnossa käytettävien palveluiden ja toimintojen sovittamiseen päätelaitteiden kesken SIP käyttää SDP (Session Description Protocol) -protokollaa. Konferenssit muodostetaan käyttäen vain niitä ominaisuuksia, joita kaikki päätelaitteet tukevat. Jos puhelun muodostaminen päätelaitteen kanssa ei jostain syystä onnistu, SIP selvittää syyn ja lähettää SIP-virhesanoman, joka kertoo, miksi yhteyttä ei saatu. Puhelun hallinta mahdollistaa uuden osallistujan liittämisen jo olemassa olevaan keskusteluun, puhelun siirtämisen päätelaitteelta toiselle ja puhelun lopettamisen päätelaitteilta yksitellen tai yhdessä. SIP tukee myös median ominaisuuksien, kuten käytettävän puhekoodekin, vaihtoa istunnon aikana. [4, s. 9; 5, s. 1-2].

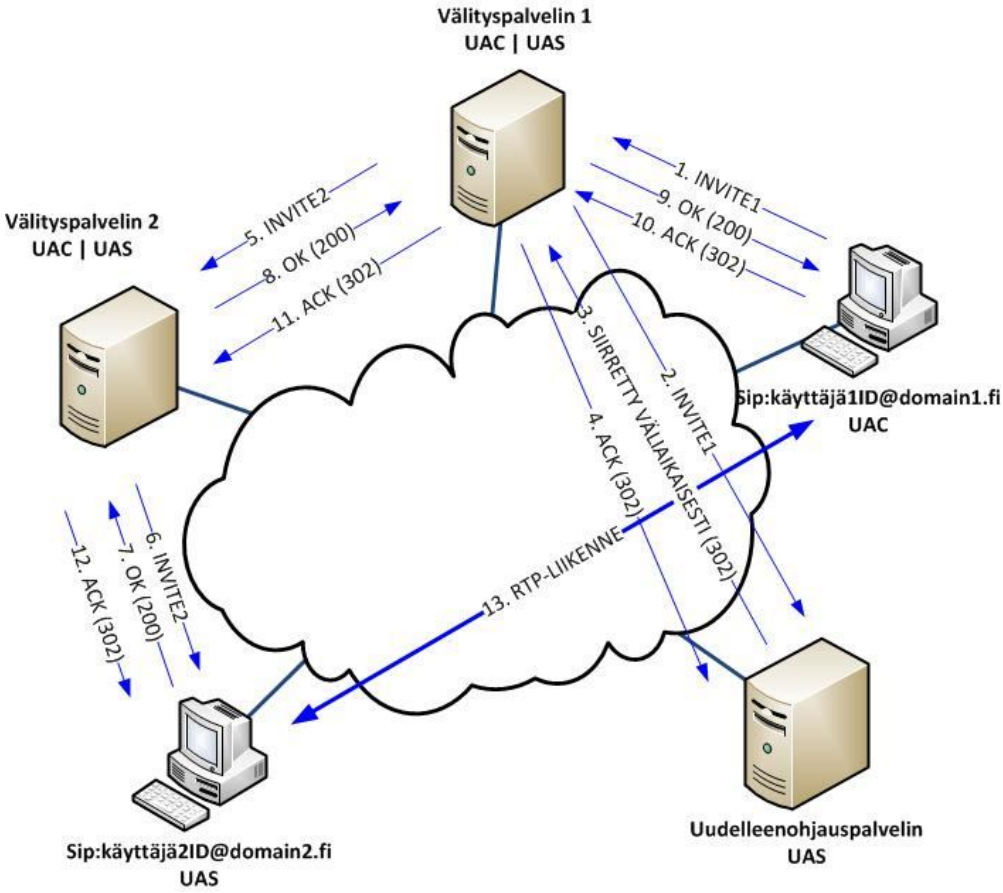
2.3.3 SIP-viestit

SIP käyttää pyyntö- ja vastaus-viestejä IP-verkon laitteiden väliseen kommunikointiin. Vastaukset voidaan yhdistää oikeisiin pyyntöihin SIP-viestin otsikossa olevien Via- ,To- ,From- ,Call-ID- ja Cseq-kenttien avulla. Pyyntöjä on kuudentyyppisiä:

- INVITE – Kutsuu käyttäjän tai palvelun istuntoon.
- ACK – Vahvistaa, että vastaus INVITE-viestiin on saatu.

- BYE – Päättää istunnon.
- CANCEL – Peruuttaa keskeneräisen SIP-operaation, mutta ei käynnissä olevia puheluita..
- OPTIONS – Kyselee palvelimien ominaisuuksia.
- REGISTER – Rekisteröi käyttäjän eli sitoo IP-osoitteen SIP-osoitteeseen.

SIP-vastausviestit on numeroitu kolmen numeron mittaisella koodilla, jotka on lajiteltu kuuteen vastausryhmään. 1xx-sarjan viestit ovat väliaikaisia tiedotuksia. Ne eivät koskaan lopeta istuntoa eli niiden jälkeen tulee aina yksi tai useampi viesti. 2xx-sarjan viestit ilmoittavat pyynnön onnistumisesta. 3xx-sarjan viestit indikoivat uudelleenohjaamisen jatkotoimenpiteitä. 4xx-viestit viittaavat virheeseen asiakaslaitteen pyynnössä. 5xx-virheet kertovat palvelimen virheestä. 6xx-sarja viittaa globaaliin virheeseen, joka ei liity yksittäiseen asiakkaaseen tai palvelimeen. Tarkempi lista SIP-vastausviesteistä löytyy liitteestä 1. [4, s. 13, 137; 5, s. 7, 28].

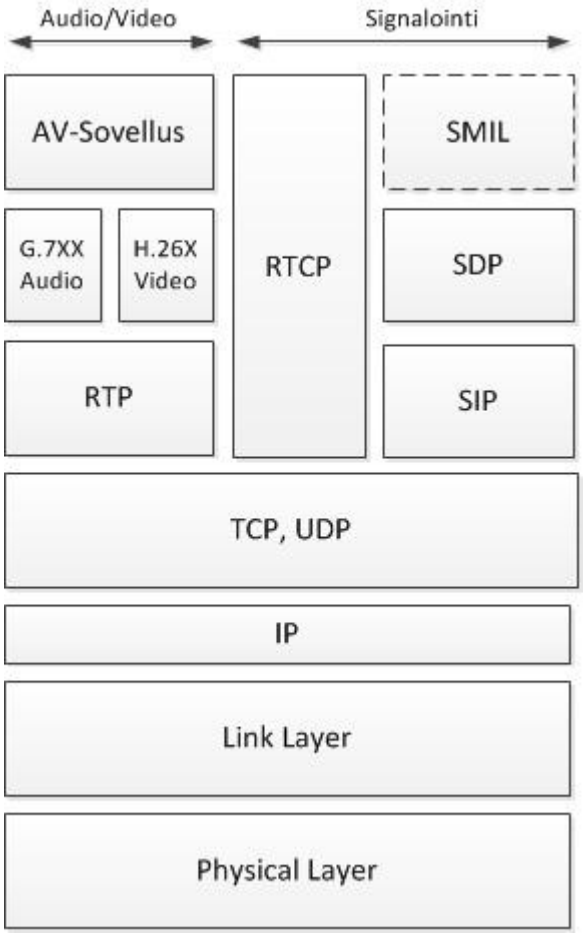


Kuva 2. Esimerkki SIP-istunnon muodostamisesta.

Kuvassa 2 on esitetty esimerkki SIP-istunnon muodostamisesta kahden käyttäjän välillä. Käyttäjät ovat eri verkoissa, joten koneiden välillä ei ole suoraa yhteyttä. Yhteyden muodostus alkaa, kun käyttäjä1:n asiakaskäyttäjäagentti (UAC) lähettää INVITE-kutsun välityspalvelin1:lle, joka puolestaan lähettää kutsun uudelleenohjauspalvelimelle, koska ei tiedä, missä käyttäjä2 sijaitsee. Uudelleenohjauspalvelin ilmoittaa, että käyttäjä on siirretty väliaikaisesti ja palauttaa seuraavan palvelimen osoitteen. Välityspalvelin1:ltä vastaa siihen ACK-kuittausviestillä. Välityspalvelin lähettää INVITE-kutsun välityspalvelin2:lle, joka sattuu tuntemaan käyttäjän2. Kun käyttäjä2 saa kutsun, se vastaa siihen myöntävästi lähettämällä OK-sanoman. Kun OK-sanoma on kulkenut verkossa käyttälle1, lähettää se vielä kuittauksen käyttäjälle2. Tämän jälkeen osapuolten välinen RTP-liikennöinti alkaa, ja se kulkee verkossa omaa reittiään. Signalointi kulkee aina käyttäjille lähimpien välityspalvelinten kautta. SIP-istunnon muodostamisen aikana viestit ovat saattaneet kulkea verkossa useammankin välityspalvelimen kautta välityspalvelin1:n ja välityspalvelin2:n välillä. Yhteyden muodostuttua SIP-viestien ei tarvitse enää kulkea kuin käyttäjille lähimpien välityspalvelinten kautta.

2.4 Muita SIP-VoIP-liikenteen protokollia

SIP-protokollan lisäksi VOIP:n toteutuksessa tarvitaan monia muitakin IP-verkon protokollia. SIP määrittelee vain merkinannon toteutukseen vaadittavan signaloinnin, eikä esimerkiksi ota kantaa siihen, miten multimedian liikennöinti hoidetaan. Median siirto tapahtuukin SIP-protokollasta riippumattomalla RTP-protokollalla, jonka kuljetuksesta UDP- ja IP-protokollat huolehtivat. Kuvassa 3 on esitetty SIP-protokolla-arkkitehtuuri.



Kuva 3. SIP-protokolla-arkkitehtuuri. [2, osa1, s. 9.]

2.4.1 IP

Internet Protocol (RFC 791) on OSI-mallin verkkokerroksen protokolla. Se sisältää osoite- ja hallintainformaatiota, joiden avulla pakettiliikenne IP-verkossa voidaan reitittää. Sen tähden se toimii perustana kaikkien pakettien

kuljettamisessa. Se mahdollistaa myös datasähkeiden pilkkomisen pienemmiksi osiksi ja uudelleenkokoamisen, jotta ne voidaan lähettää erilaisia MTU (Maximum Transmission Unit) -arvoja tukevien datayhteyksien kautta. [7.]

2.4.2 TCP ja UDP

Transmission Control Protocol (RFC 793) on kuljetuskerroksen yhteydellinen protokolla, joka takaa datan kuljetuksen luotettavuuden IP-verkossa. TCP mahdollistaa mm. pakettien saapumisen perille oikeassa järjestyksessä, ruuhkanhallinnan sekä kadonneiden pakettien uudelleenlähetyksen. Yhteydellisenä protokollana TCP muodostaa yhteyden päätelaitteiden välille ennen varsinaisen datan siirtoa ja purkaa yhteyden sen jälkeen. Koska signalointi on kriittistä dataa, sen kuljettamiseen käytetään tavallisesti TCP-protokollaa. [7.]

User Datagram Protocol (RFC 768) on yhteydetön kuljetuskerroksen protokolla, joka ei takaa pakettien perillemenoa eikä ruuhkanhallintaa, mutta on sen sijaan kevyt protokolla, joka soveltuu hyvin reaaliaikaisen datan, kuten IP-puheen kuljettamiseen. Sekä TCP että UDP käyttävät porttinumeroita ohjaamaan tiedonkulkua oikeiden sovellusten välillä. [7.]

2.4.3 RTP ja RTCP

Real Time Protocol (RFC 3550) on reaaliaikaisen datan siirtoon suunniteltu istuntokerroksen protokolla, joka on riippumaton kuljetus- ja verkkokerroksen protokollista. RTP tarjoaa median tyypin tunnistuksen, järjestysnumeroinnin, aikaleimat ja liikenteen tarkkailun. RTP koostuu kahdesta osasta: RTP ja RTCP. RTP:n kuljettaessa dataa, jolla on reaaliaikaiset ominaisuudet, tarkkailee RTCP (Real Time Transport Protocol) yhteyden laatua sekä välittää osallistujatietoja. [8, s. 12, 15.] Jokaiselle yksittäiselle RTP:n kuljettamalle medialle laitteessa määritellään oma UDP-porttinumero, joilla esimerkiksi useat yhtäaikaiset puhelut erotellaan [2, osa 3, s. 20].

2.4.4 SDP

Session Description Protocol (RFC 4566) kuvaa istunnon ominaisuudet. Sen avulla istuntoon osallistuville päätelaitteille ilmoitetaan median yksityiskohdat, kuten median tyyppi, kuljetusprotokolla ja median formaatti, osoitteet ja portit sekä muu mahdollinen istuntoa kuvaava metatieto. Istuntokerroksen

protokollana SDP-protokolla tarvitsee alleen siirtoprotokollan, kuten SIP:n, SAP:n (Session Announcement) tai RTSP:n (Real Time Streaming Protocol). [9, s. 2, 5.]

2.4.5 SMIL

Synchronized Multimedia Integration Language (SMIL) on W3C:n kehittämä XML-pohjainen kuvauskieli, jonka avulla voidaan luoda interaktiivisia ja reaaliaikaisia multimediaistuntoja, kuten multimediaesityksiä erilaisten mediaelementtien (kuva, ääni, video) avulla. Mediaelementit voivat sisältää hyperlinkkejä, ja esitykset voidaan kuvata näytöllä. SMIL:in syntaksia voidaan käyttää muissakin XML-pohjaisissa kielissä, erityisesti synkronisoinnin ja ajoituksen esittämiseen. [10.]

2.5 VoIP-liikenne verkossa

Reaaliaikainen media on aikakriittistä. Jos esimerkiksi IP-puhelun aikana sekunninmittainen pätkä puhetta katoaa verkkoon, eikä saavu oikeaan aikaan perille, on sen hyöty menetetty ja palauttaminen tekisi vain lisää haittaa. Hyvän laadun takaamiseksi VoIP-liikenne vaatii verkolta riittävää siirtokapasiteettia ja viiveen sekä sen vaihtelun pienenä pysymistä. Pakettien on kuljettava päätepisteiden välillä riittävän nopeasti ja melko tasaista vauhtia, jotta puhe olisi hyvänlaatuista.

2.5.1 Kaistan kulutus

Yhdelle IP-puhelulle tarvittava tiedonsiirtokapasiteetin tarve määräytyy käytettävän koodekin, paketoitavan puhenäytteen pituuden, protokollien otsikkokenttien, siirtoyhteyskerroksen protokollan ja mahdollisen tunnelointiprotokollan perusteella. Paketoitavan puhenäytteen pituutta muuttamalla voidaan tasapainotella hyvän laadun ja kaistankulutuksen väillä Pitkillä puhenäytteillä kaistan kulutus pysyy alhaisena, mutta äänenlaatu on huono pitkien viiveiden takia. Lyhyiden puhenäytteiden tapauksessa laatu on hyvä, jos tiedonsiirtokapasiteetti on riittävä.

Esimerkiksi 8 kHz:n taajuudella näytteistävä ja äänidataa 64 kbps kehittävä G.711-koodekki saa 20 ms:n aikana otettua 160 kpl 8 bitin näytteitä, mistä seuraa 160 tavua dataa. Tähän liitetään RTP-kehys, joka on 12 tavua, UDP-kehys, joka on 8 tavua ja IP-kehys, joka on 20 tavua, jolloin yhden IP-paketin kooksi tulee 200 tavua. Siirtoyhteyskerroksen protokollan ollessa linkkikoh-

tainen, saattavat IP-paketit joutua kulkemaan eri protokollien välityksellä, joista Ethernet vie 18 tavua, Frame Relay 6, MLP 6 ja 802.1Q 22 tavua [12.]. Ethernetin yli kulkevan G.711- koodekkia käyttävän puheliikenteen aiheuttama kuorma olisi siten 87,2 kbps (218 t * 50 fps * 8 bit/t). Mahdollisen IPSEC:in tai tunnelointiprotokollan käyttö tarkoittaa aina uusien protokollaotsakkeiden mukaantuloa, mikä kasvattaa lähetettävien pakettien kokoa ja siten kaistan kulutusta. IPSEC:ssä käytettävä tiedon salaus kasvattaa myös paketin kokoa riippuen käytettävistä autentikointi- ja salausalgoritmistä, sekä IPSEC:n tilasta (kuljetustila, tunnelitila).

Pakettikohtaisen puhenäytteen ollessa 20 ms, on sekunnissa lähetettävä 50 pakettia. Mikäli puhenäytteen pituus puolitetaan, on pakettien lähetystaajuus kaksinkertaistettava. Varsinaisen äänidatan kaistankulutus suhteessa koko siirrettävän datan kaistankulutukseen laskee, mikä aiheuttaa kaistankulutuksen kasvun ja hukkuneiden pakettien määrä periaatteessa kasvaa. Jos puhenäytettä sitä vastoin pidennetään, kasvattaa paketointiprosessi viivettä. [12.]

2.5.2 Viive, viiveen vaihtelu ja pakettien katoaminen

Pakettikytkentäisen verkon perusperiaatteellinen tapa käsitellä paketteja tasa-arvoisesti ei ole paras mahdollinen reaaliaikaisen datan siirtoon. Kun verkossa on ruuhkaa ja paketit joutuvat jonottamaan reititystä, kasvavat viiveet usein reaaliaikaisen liikenteen kannalta liian suureksi. Paketit saattavat kulkea verkon yli myös useaa eri reittiä, joissa eri linkkien välimatkat ja nopeudet vaihtelevat. Nämä yhdessä aiheuttavat myös pakettien eriaikaista perille saapumista, jota kutsutaan viiveen vaihteluksi. Sekä viive, että viiveen vaihtelu ovat ihmiskorvalla helposti kuultavissa ja mikä heikentää puhelun laatua.

Viivettä voidaan mitata sekä yksisuuntaisesti että kaksisuuntaisesti. Kaksisuuntainen viive on se aika, joka kuluu, kun paketti kulkee verkossa määränpäähänsä ja tulee takaisin. ITU-T:n G.114-suositus tarkastelee äänisovellusten viiveitä [13]. Suositus sisältää seuraavanlaiset määritykset viiveille (Taulukko 2).

Taulukko 2. ITU-T/G.114:n suositukset viiveille. [13]

Viive (ms)	Kuvaus
0-150	Sopii useimmille käyttäjäsovelluksille.
150-400	Soveltuvuus edellyttää, että järjestelmänvalvoja tiedostaa viiveen vaikutuksen sovellusten tiedonsiirron laatuun.
yli 400	sopimaton yleisen verkkosuunnittelun mukaisiin tavoitteisiin

Koska digitaaliset ääni- ja videopaketit täytyy purkaa samoilla koodekeilla ja toistaa samassa järjestyksessä ja samalla nopeudella kuin ne on luotu, ei yksittäisiä viipyviä paketteja voida kovin kauaa odotella. Puskuroinnilla voidaan vaikuttaa ruuhkaan, viiveisiin ja viiveen vaihteluun tiettyyn rajaan asti. Kun raja ylittyy, on paketin sisältämä ääninäyte merkityksetön. Tällöin paras ratkaisu on paketin hylkääminen. Yksittäisen paketin sisältämän ääninäytteen (esim. 20ms) katoaminen ei vielä vaikuta puheen laatuun käytännössä, mutta riittävän suuri määrä kadotettuja paketteja aiheuttaa aukkoja puheessa.

2.5.3 QoS

Ilman QoS- menetelmiä, kaikki liikenne verkossa on samanarvoista. Liikenteen käsittelyssä puhutaan tällöin termistä ”Best Effort”. Mikäli liikenteessä on ruuhkaa, joutuvat myös paketit jonottamaan verkkolaitteiden puskurimuisteissa, eivätkä esimerkiksi reaaliaikaisen liikenteen paketit pääse muita paketteja nopeammin perille. Ongelma voi kaataa esimerkiksi koko VoIP-puhelun.

Quality of Service (QoS) ei suoraan tarkoita palvelun laatua, mutta määrittelee tekniikoita, joilla vaikutetaan verkkoliikenteen kulkuun ja sitä kautta laatuun halutussa verkon osassa. Laatua voidaan lähteä toteuttamaan joko ennaltaehkäisevin keinoin tai puuttua asiaan vasta kun tilanne on jo päällä. Tekniikat voidaan jaotella karkeasti kahteen osaan: Integrated Services (IS) ja Differentiated Services (DS). Pääasiallinen ero on se, että IS valmistelee reitin vaadittujen QoS-parametrien mukaiseksi ennen varsinaisen liikenteen alkamista ja takaa pysyvän tiedonsiirtonopeuden. DS luokittelee liikennettä sen kiireellisyyden mukaan ja on hyvin skaalautuva, mutta ei takaa laatua eikä varaa kaistaa etukäteen, kuten IS.

QoS:n toteuttamisesta vastaa yleensä verkon omistaja itse. Esimerkiksi yritys voisi määritellä miten palvelun laatu sen omassa verkossa toteutetaan. Sama pätee myös isoihin operaattoreihin, joiden omistuksessa isot runkoverkot ovat. Mikäli QoS haluttaisiin toteuttaa internetin yli, siitä pitäisi siis sopia operaattorin kanssa. Lähiverkossa palvelun laatua voisi toteuttaa esimerkiksi liikenteen luokittelun Cos (Class of Service) avulla. Viiveille herkälle VoiP-liikenteelle annettaisiin muuta liikennettä korkeampi prioriteetti, jolloin verkkolaitteet käsittelisivät näitä paketteja niille suoduin etuoikeuksin.

Ongelmia voidaan ennaltaehkäistä myös verkon riittävällä redundanttiosuudella. Laitteiden ja linkkien määrä voitaisiin toisaalta ylimitoittaa, mutta myöskään yhtäaikaisten puheluiden rajoittaminen sopivaan määrään ei ole huono ratkaisu.

2.5.4 VAD

Voice Activity Detection on DSP:n tai sen tehtävää hoitavan prosessorin ominaisuus, joka tunnistaa puheen läsnäolon äänisignaalissa. Sen avulla voidaan vähentää kaistankulutusta ja prosessointikuormaa jättämällä ”hiljaiset” eli puheettomat kohdat pois jatkokäsittelystä. Kaikista mikrofonin tuottamista äänisignaaleista koodataan vain puhetta sisältävä osuus, jolloin ei myöskään synny hiljaisia paketteja, jotka muutoin kulkisivat turhaan verkon yli toiseen päähän prosessoitavaksi. Täydellinen hiljaisuus toteutuu harvoin, joten DSP on myös suunniteltu erottelemaan puhe taustamelusta. Tietyn tyyppisen ja riittävän voimakkaan taustamelun VAD saattaa kuitenkin tulkita puheeksi ja päästää läpi.

VAD:n hyödyntämiä ”hiljaisia” kohtia löytyy eri syistä. Normaalissa puhelinkeskustelussa ei tavallisesti puhuta koko aikaa päälletysten, vaan toisen puhuessa toinen yleensä kuuntelee. Sama tilanne toteutuu myös jonotustilanteessa jonotusmusiikkia kuunneltaessa. Puheen koodaus ja pakettien lähetys kuuntelijan päästä on turhaa. Myös puhujan puheessa on tavallisesti aukkoja, jotka voidaan jättää pois.

3 TIETOTURVA

Vaikka SIP-sovellukset ovat osittain hyvinkin monipuolisia ja niiden yhteensopivuus eri valmistajien välillä on hyvä, ei turvallisuutta pidä kokonaan unohtaa. SIP-järjestelmät ovat monestakin syystä haavoittuvaisia sekä yleisille pakettikytkentäisen verkon hyökkäyksille että vain SIP:lle tarkoitetuille hyökkäyksille. SIP:n toiminta yhdessä muiden protokollien kanssa muodostaa monimutkaisen kokonaisuuden, joka käyttää signalointiin tekstipohjaisia viestejä, joita ei oletusarvoisesti salata. Näin ollen tietoturvasta huolehtiminen SIP-protokollaa käytettäessä on olennaisen tärkeätä, mikäli järjestelmä halutaan pitää luotettavana ja puhelut suojattuna.

3.1 Haavoittuvuuksia

Tässä on esitelty muutamia haavoittuvuuksia, joita SIP-järjestelmät saattavat sisältää. [14.] Yhteistä näille haavoittuvuuksille on se, että ne voidaan estää tehokkaasti käyttämällä asiaankuuluvaa suojausmenetelmää, josta kerrotaan luvussa 3.2.

3.1.1 Rekisteröinnin kaappaus

Rekisteröinnin kaappaus perustuu päätelaitteen asiakaskäyttäjäagentin imitoimiseen. Hyökkääjä esittää olevansa laillinen asiakaskäyttäjäagentti ja korvaa sen IP-osoitteen omallaan. Tällöin kaikki saapuvat puhelut kulkevat hyökkääjälle. SIP-viesteissä yleisesti käytetyn UDP-protokollan salaamattomuus mahdollistaa edellä mainitun kaltaisen hyökkäyksen helposti, koska UDP:n yhteydetön ja epäluotettava menetelmä ei valvo pakettiliikennettä. Yleistä on myös yhteyden heikko suojaaminen, joka perustuu lähinnä käyttäjätunnus ja salasana –pariin. Käyttäjätunnuksia voidaan selvittää käyttäjätunnuksia vakoilemalla ja salasanoja kokeilemalla. Puheluiden lisäksi hyökkääjä voi päästä käsiksi tärkeisiin tunnistautumis- tai signalointitietoihin. Liikenne ei välttämättä pysähdy hyökkääjän käyttäjäagenttiin, vaan voi myös

kulkea sen läpi. Tällöin hyökkääjä voi kerätä ja muuttaa sekä signalointia että mediaa aidon UAC:n ja UAS:n välillä.

3.1.2 Hyökkääjän välityspalvelin

Onnistuneella välityspalvelimen imitoinnilla hyökkääjän on mahdollista huijata useaa asiakas- ja palvelinkäyttäjäagenttia, päästä käsiksi kaikkiin SIP-viesteihin ja saada molempiin suuntiin kulkevista puheluista täysi hallinta. Hyökkääjä voi huijata nimipalvelua (DNS) sekä vaihtaa ARP-reititystietoja (ARP cache), minkä jälkeen puhelut menevät hyökkääjän haluamaan paikkaan. Tämän jälkeen puheluita voidaan salakuunnella, manipuloida, liittää tai erotella ja nauhoittaa.

3.1.3 Viestien peukalointi ja puhelun häirintä

Viestien peukaloinnissa on kyse viestien kaappaamisesta ja sen jälkeen suoritettavasta sisällön muuttamisesta. Se voidaan toteuttaa sekä edellä mainituilla tavoilla, että monella muulla tapaa. Perusedellytyksenä voidaan kuitenkin pitää pääsyä sellaiseen verkkolaitteeseen tai rooliin verkossa, joka mahdollistaa SIP-viestien käsittelyn. Näitä laitteita ovat mm. välityspalvelin, palomuuri ja yhdyskäytävä.

Puheluita voidaan myös häiritä lähettämällä oikein muotoiltuja SIP-sanomia käyttäjäagenteille. Esimerkiksi BYE-sanoman lähettäminen käyttäjäagenteille, katkaisee puhelun. RE-INVITE-viesteillä puheluita voidaan ohjata vahingollisesti vääriin osoitteisiin ja niitä voidaan käyttää DoS-hyökkäysten välineenä.

3.1.4 DoS (Denial of Service)

Yksi suojaamattoman järjestelmän heikkous on alttius palvelunestohyökkäyksille (DoS). Kun verkon osat käsittelevät kaikki SIP-viestit, se voidaan kaataa eli tukkia suurella määrällä viestejä. Hyökkäys voi koostua esimerkiksi INVITE- tai REGISTER-viesteistä ja se voidaan kohdistaa haluttuihin verkon osiin tai laitteisiin. Esimerkiksi palomuuriin kohdistetulla DoS-hyökkäyksellä saatetaan pyrkiä estämään palomuurin normaali toiminta ja siten heikentämään sen tarjoamaa suojaa.

3.2 Liikenteen turvaaminen

SIP:n turvallisuus perustuu lähtökohtaisesti IP:n ja VoIP:n turvaominaisuuksiin. Oikein valitut protokollat ovat yksi tapa vaikuttaa tietoturvaan. Signaloinnin kuljetus TCP-protokollaa käyttäen parantaa tietoturvaa. TCP:n ominaisuudet, kuten yhteyden avaaminen ja sulkeminen (yhteydellinen protokolla), pakettien järjestysnumerot ja kadonneiden pakettien uudelleenlähettäminen, tekevät TCP-pakettien huijaamisesta UDP-pakettien huijaamista vaikeampaa.

SIP:n tietoturvaa voidaan entisestään parantaa tiedonsalausprotokollan avulla. Yleisesti tietoliikenteessä käytetty TLS (Transport Layer Security) –protokolla (RFC 2246) tarjoaa vahvan salauksen ja autentikoinnin SIP-komponettien väliseen signalointiin. TLS kapseloi ylemmän tason protokollat ja käyttää symmetristä salausta, jossa käytettävät yhteyskohtaiset salausavaimet tekevät yhteydestä luotettavan. TLS on kehitetty SSL v. 3.0:n pohjalta.

Mediansiirron turvallisuudesta vastaamaan voidaan käyttää Secure RTP (SRTP) –protokollaa (RFC 3711) , joka varmistaa RTP- ja RTCP-pakettien autentikoinnin, salauksen ja eheyden SIP-päätelaitteiden välillä. SRTP on RTP-protokollan profiili, joka sijaitsee sovelluskerroksen ja verkkokerroksen välissä. Se käyttää valmiita standardeja avaintenhallintaan ja muihin toiminnallisuuksiin. Pakettien salaukseen käytetään oletusarvoisesti Advanced Encryption Standard (AES) –algoritmia ja symmetrisiä salausavaimia.

Yhtenä vaihtoehtona voidaan nähdä myös Virtual Private Netvork (VPN) –tunnelointi, jolloin kaikki liikenne päätepisteiden välillä siirretään salattuna. Tunnelointia käytetään yhdistämään tietoturvallisesti niin yksittäisiä laiteita kuin lähiverkkojakin turvattoman verkon, kuten internetin yli. VPN-tekniikoita ovat muun muassa. IPSec, L2TP ja PPTP

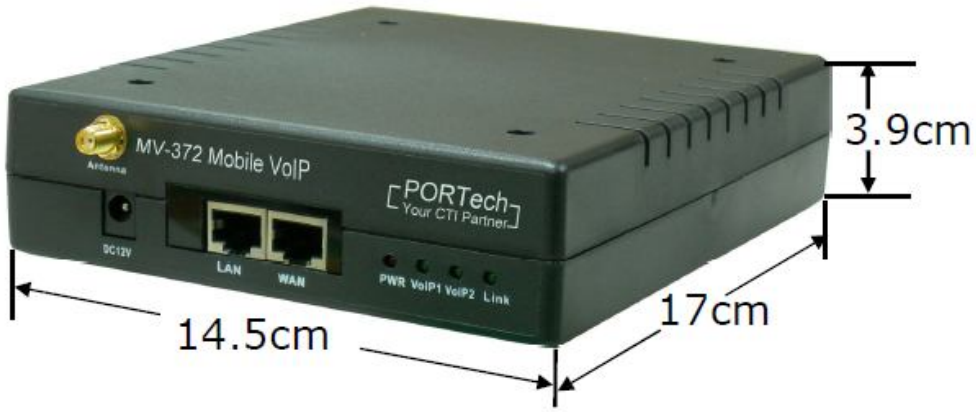
Turvallisuusstandardia käytettäessä, sen toteuttaminen kaikissa järjestelmän laitteissa on tärkeää, sillä yksikin suojaamaton laite vaarantaa koko järjestelmän. Laitteet tulisi siis valita siten, että ne tukevat haluttuja standardeja.

4 OHJELMISTOT JA LAITTEISTOT

Tässä osiossa esitellään pääpiirteittäin työssä käytetyt laitteet, ohjelmistot ja niiden käyttötarkoitus. Yhtä laitetta käytettiin pelkästään yhdyskäytävän ominaisuudessa ja kolme VoIP-järjestelmää ohjaamaan suunniteltua VoIP-palvelinta toimi lähinnä puhelinvaihteen roolissa. Työssä järjestelmään asennettiin muutama pöytämallin IP-puhelin, joista osa oli samanlaisia Ciscon malleja. Niiden lisäksi asennettiin X-Lite-ohjelmistopuhelin Windows-käyttöjärjestelmään. Pöytäpuhelinten samankaltaisuudesta johtuen esiteltäväksi valittiin vain yksi malli: Cisco 7960.

4.1 Portech MV-372

GSM-VoIP-yhdyskäytävänä työssä toimi Portech MV-372, joka tarjoaa kaksi puhekanavaa ja kaksi verkkoliitäntää: LAN (Local Area Network) ja WAN (Wide Area Network), joista LAN-verkossa se voi toimia DHCP-palvelimena. Portech tukee puheluiden reititystä GSM-verkosta VoIP-verkkoon ja toisinpäin. VoIP-puheluissa laitteen toiminta perustuu SIP-protokollaan, jota käyttäen se on yhteensopiva ainakin Asterisk, Trixbox, 3CX ja VoIPBuster–palvelinten kanssa. Tuettuja mobiiliverkon kanavointitekniikoita ovat TDMA, CDMA ja WCDMA. MV-372 tukee ketjuttamista, mikä mahdollistaa useiden yhdyskäytävien liittämistä yhdeksi klusteriksi. Laitteeseen saa lisävarusteena myös erillisen SIM-korttipankin. Myös tekstiviestien lähettäminen mobiiliverkon laitteisiin on mahdollista.



Kuva 4. GSM VoIP -yhdyskäytävä

4.2 Trixbox CE@Dell Power Edge 850

Yhtenä VoIP-palvelinohjelmistona toimi Dell Power Edge 850-palvelimeen jo valmiiksi asennettuna ollut Trixbox CE (Community Edition) -ohjelmisto. Trixbox on Asterisk-distribuutio, aiemmalta nimeltään Asterisk@Home, jonka Andrew Gillis aloitti vuonna 2004. Trixbox CE on ilmaisversio, joka perustuu GNU:n avoimeen lähdekoodiin (GPL General Public License). Se rakentuu pienistä ohjelmapaketeista, jotka yhdessä muodostavat Trixbox-nimisen ohjelmiston. Ohjelmiston LAAMP (Linux®, Apache™, Asterisk®, mySQL®, ja PHP) rakenne mahdollistaa helpon käytettävyyden web-pohjaisen käyttöliittymän avulla. Käyttöjärjestelmänä toimii Red Hat Enterprise Linuxiin perustuva CentOS ja web-palvelimena Apache. Web-hallintasivut on toteutettu PHP:lla, tietokannat MySQL-järjestelmällä ja puhelunohjaustoiminnot perustuvat suosittuun Asterisk-puhelinvaihdeohjelmistoon. Asetusten konfiguroimisen graafisen web-käyttöliittymän avulla mahdollistaa Trixboxiin kiinteästi kuuluva FreePBX GUI (graphical user interface).

Avoimen lähdekoodin ansiosta Trixboxin toiminnallisuus on lähes rajaton, sillä uusia kolmannen osapuolen ohjelmia sovitetaan RPM:lle (Red Hat Packet Manager) jatkuvasti.

Trixboxista on myös kaupallinen PBXtra-teknologiaan perustuva versio trixbox Pro, joka on tehty ilmaisversiota paremmin suuriin asennuksiin skaalautuvaksi, vaikka perustuukin CE:n kanssa samoihin peruskomponentteihin. Pro version web-hallintapaneeli ja kommunikointiohjelma HUD Pro eivät ole kuitenkaan avoimen lähdekoodin ohjelmia, joten eroavaisuuksia käyttämisen puolellakin on.

Kuva 5. Dell Power Edge -räkkipalvelin.

4.3 Cisco Call Manager

Cisco Call Manager on osa Ciscon IP-puheliikenteeseen suunnittelemaa järjestelmää, joka tunnetaan nimellä Cisco IP Communications. Call Manager on ohjelmistopohjainen ratkaisu IP-puheluiden prosessointiin perustuen Ciscon AVVID-arkkitehtuuriin (Architecture for Voice, Video and Data). Se koostuu useista integroiduista puhesovelluksista ja apuohjelmista toimien pakettimuotoisen puheliikenteen keskuksena. Sen kautta voidaan yhdistää muun muassa IP-puhelimet, VoIP-yhdyskäytävät, multimediasovellukset ja mediaprosessointilaitteet. AVVID-arkkitehtuuri mahdollistaa Call Managerien yhdistämisen yhtenä kokonaisuutena hallittavaksi klusteriksi ja edelleen klustereiden kokoamisen vielä suuremmiksi kokonaisuuksiksi.

Työssä käytetty Call Managerin ohjelmistoversio 4.1 oli melko vanha. Siitä johtuen sen toiminnallisuus SIP:n osalta oli melko vaatimatonta verrattuna esimerkiksi Trixboxiin, perustuen lähinnä trunk-linkkien kautta muodostettuihin yhteyksiin. Uudemmat Cisco Unified Communications manager- tuotteiden SIP-tuki on parempi. Call Manager oli asennettuna ATX-mallin tietokonekoteloon.

Kuva 6. Cisco Call Manager.

4.4 Cisco Unified Communications 520

Eräs Ciscon VoIP-ratkaisu pieniä yrityksiä silmällä pitäen on Unified Communications 520 –VoIP-palvelin, joka tarjoaa puhe- , data- ja videosiirron lisäksi puheluiden ohjauksen. Myös integroituminen erilaisten työpöytäohjelmien, kuten sähköposti ja kalenteri, kanssa on mahdollista. Ciscon suunnittelema kompaktin kokoinen laite sisältää Ciscon IOS-ohjelmistoon pohjautuvan reitittimille suunnitellun Call Manager Express -ratkaisua laajemman kokonaisuuden, joka sisältää puheluiden ohjauksesta vastaavan Cisco Unified Communications Manager Express (Unified CME) -ohjelmiston, ääniviesteistä ja automaattisesta avustajasta vastaavan Cisco Unity Express -ohjelmiston sekä turvallisuudesta ja palomuurista vastaavan ohjelmiston. Laite sisältää Liitäntöjä laitteesta löytyy seuraavasti: 10/100 Mbps ethernet-portti, 10/100 Mbps ethernet-laajennusportti, kahdeksan 10/100 PoE (Power over Ethernet) –liitäntää lähinnä IP-puhelimia varten, neljä analogista FXS-porttia kautta ja kaksi digitaalista BRI-porttia. Ethernet-portti on tarkoitettu ulkoverkkoon esim. internetiin kytkemistä varten ja se on eri verkossa kuin 8 PoE-porttia, joihin kytketyt puhelimet voivat saada IP-osoitteensa UC520:n DHCP-palvelimelta. IP-osoitteiden lisäksi puhelimet voivat ladata ohjelmistonsa palvelimelta. [14].

Kuva 7. Cisco UC520 [15].

4.5 Cisco 7960 –ip-puhelin

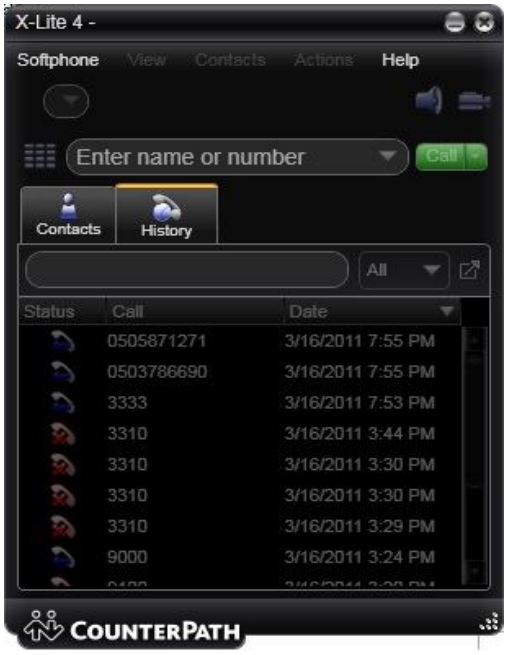
Ciscon lippulaivamallistoon (7900-sarja) kuuluva bisnes-malli 7960 soveltuu SIP-puheluiden lisäksi puheluiden ohjaamiseen. Puheluita voi esimerkiksi asettaa pitoon, uudelleenohjata ja yhdistää uuteen numeroon. Se tukee myös XML-kielellä toteutettuja web-pohjaisia sovelluksia, kuten erilaiset tiedotepalvelut. Suuri näyttö välittää informaatiota selkeästi. Hakemistopalvelu säilyttää puhelutietoja niiden iän ja käytön mukaan.

Kahden RJ-45-liitännän ansiosta, puhelimen voi kytkeä tietokoneen ja kytkimen väliin, jolloin puhelin huolehtii oman kaistatarpeensa riittävyydestä tietokoneen rinnalla. Puhelin hakee IP-osoitteen DHCP:n avulla ja voi ladata uusimman ohjelmistopäivityksen palvelimelta TFTP:tä käyttäen.

Kuva 8. Cisco 7960 IP-puhelin.

4.6 X-Lite 4 -ohjelmistopuhelin

X-Lite 4 -ohjelmistopuhelinta käytettiin selvittämään internetin mahdollista vaikutusta VoIP-puheen laatuun. X-Lite on Counterpath-yhtiön ilmainen ohjelmistopuhelin, jolla on kaksi maksullista sisarmallia: Eyebeam ja Bria. X-lite on reilusti karsittu malli, eikä tue esimerkiksi useampaa linjaa, konferenssipuheluita, salausta tai HD-videota. X-lite tukee kuitenkin SIP-puheluita videon kera sekä peräti 11 äänikoodekkia, joista oletusarvoisesti aktivoituna ovat Broadcomin BroadVoice-32 ja G.711 alaw/ulaw. Erikoista on, että X-Lite ilmoittaa bittinopeudeksi G.711-koodekille 80000 bps. Videokoodekkina X-litessä on H.263 ja H.236+.



Kuva 9. X-Lite-ohjelmistopuhelin.

5 LAITTEIDEN HALLINTA

Tässä osassa tarkastellaan yhteysmenetelmiä ja -protokollia, joita työssä käytettiin laitteiden hallintaan ja asetusten konfiguroimiseksi. Kaikkiin laitteisiin ei otettu yhteyttä samalla tavalla, eikä yksi menetelmä laitetta kohti aina riittänyt pääsemään toivottuun lopputulokseen.

5.1 DHCP

Domain Host Configuration Protocol (RFC 2131) kuvaa menetelmän, jolla TCP/IP-verkon laitteille voidaan siirtää ja asettaa konfiguraatiotietoa. DHCP perustuu vanhempaan BOOTP-protokollaan. DHCP:tä käytetään yleisesti

IP-osoitteiden automaattiseen jakamiseen verkon päätelaitteille. Toiminta perustuu palvelin-asiakas-malliin, jossa palvelin lainaa IP-osoitteen asiakkaalle joko toistaiseksi tai ennalta määritetyksi ajaksi. Tämä helpottaa laitteiden käyttöä verkossa, sillä se ei vaadi käyttäjän puuttumista toimiakseen. Mikäli laitteella on yhteys verkkoon, hakee se IP-osoitteen yleensä jo käynnistyessään. Tässä työssä käytetyt puhelimet saivat IP-osoitteen oletusarvoisesti DHCP-palvelimilta. UC520 toimi dhcp-palvelimena siihen kytketyille puhelimille.

5.2 HTTP ja HTTPS

Hyper Text Transfer Protocol mahdollistaa asiakaskoneen selaimen ja palvelinkoneen välisen yhteyden, jossa palvelin vastaa selaimen kautta lähetettyihin pyyntöihin. Selaimen kautta voidaan siirtää monipuolista sisältöä, kuten kuvia, videota, ääntä ja tiedostoja. Tavallisesti HTTP:tä käytetään websisällön välittämiseen palvelimelta selaimelle. HTTP käyttää TCP/UDP-porttia 80.

HTTPS lisää liikenteen salauksen http-protokollaan. Salaus tapahtuu SSL- tai uudemman TLS-protokollan avulla. SSL käyttää yhteyksissä varmenteita ja salaa tiedon symmetrisesti ennen lähetystä. HTTPS:n käyttämä TCP/UDP-portti on 443.

Tässä työssä http- ja https-protokollia käytettiin web-pohjaisilla hallintasivuilla toteutettujen laitteiden konfiguroimiseen. GSM-VoIP-yhdyskäytävä tuki ainoastaan web-pohjaista konfigurointia ja HTTP-yhteyttä. Osa puhelimista tuki molempia protokollia, osa vain http:tä. UC520 ja Trixbox tukivat https-yhteyttä.

5.3 Telnet

Telnet on vanha ja hyvin laajalti tuettu kaksisuuntainen pääteyhteysprotokolla, joka mahdollistaa esimerkiksi palvelinten tai verkkolaitteiden konfiguroimisen komentorivipohjaisesti. Telnet ei ole tietoturvallinen, sillä yhteys on salaamaton ja liikenne kulkee verkossa selkokielisenä tekstinä. Siksi Telnettiä voi suositella käytettäväksi ainoastaan tunnetuissa lähiverkoissa, joissa ei ole tietoturvauhkaa. Julkisen verkon yli kulkeviin pääteyhteyksiin suositellaan käytettäväksi Telnetin sijaan jotain salattua pääteyhteyttä.

5.4 SSH

SSH on Telnetin tavoin verkkoprotokolla pääteyhteyksien muodostamiseen, mutta se tarjoaa myös käyttäjän tunnistuksen ja tiedon salaamisen julkisen avaimen menetelmällä. Yhteys perustuu asiakas-palvelin-suhteeseen, jossa asiakasohjelma ottaa yhteyden palvelimeen. Asiakas tunnistautuu palvelimelle joko salasanalla tai automaattisen yhteydenmuodostuksen mahdollistavalla julkiseen avaimeen perustuvalla tunnistautumisella. Ilmaisia SSH-ohjelmia löytyy ainakin Windowsille, Linuxille ja Macille. Tässä työssä käytettiin Putty-nimistä asiakasohjelmaa SSH-yhteyden luomiseksi Cisco UC520-laitteen komentoliittymään.

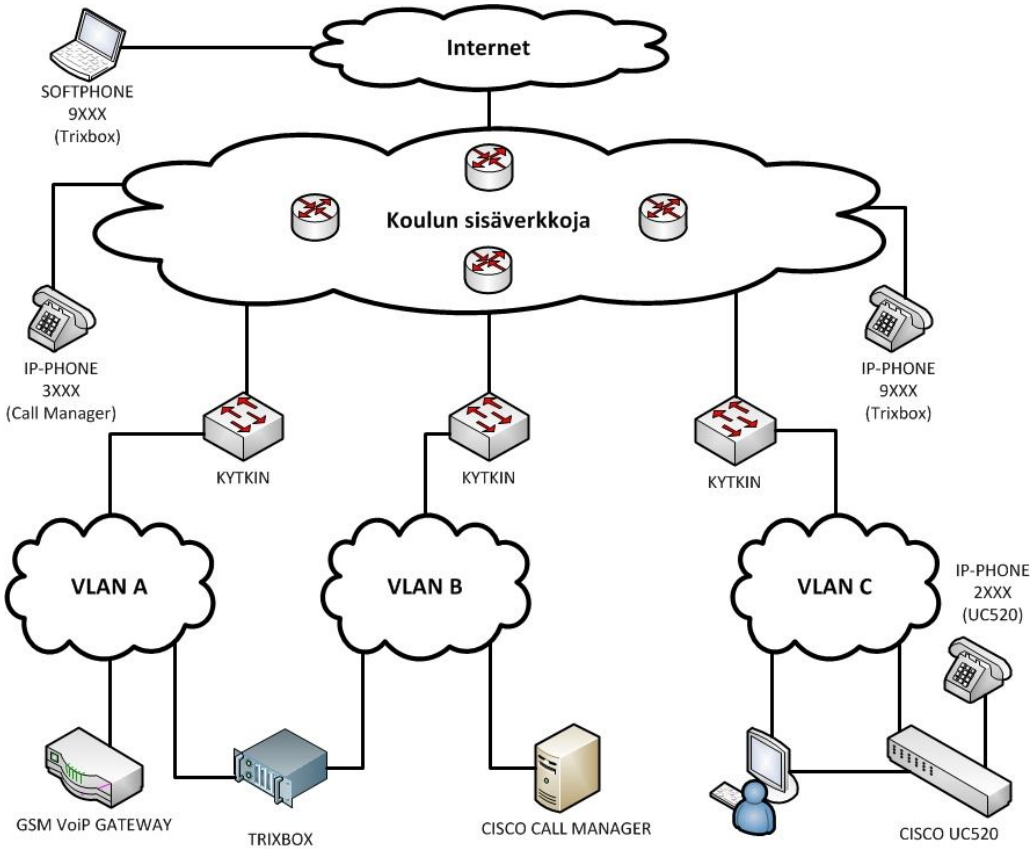
5.5 UltraVNC

Call Mangerin konfigurointi tapahtui UltraVNC-ohjelmalla toteutetun etäyhteyden avulla. UltraVNC on ilmainen VNC (Virtual Networking Protocol) –protokollaa käyttävä GNU-lisenssin alainen ohjelma, joka mahdollistaa tietokoneen etähallinnan. UltraVNC:ssä on kaksi osaa: palvelinosa VNCServer ja asiakasosa VNCWiever. Yhteys toimii siten, että Wiever-osa ottaa yhteyden Server-osaan ja kirjautuu sisään. Sen jälkeen palvelinkonetta voidaan hallita graafisen käyttöliittymän kautta. UltraVNC:ssä on monia valinnaisia lisäosia eli plugineita toiminnan parantamiseksi ja monipuolistamiseksi. Myös yhteyden salaus perustuu lisäosan asentamiseen. Myös muita VNC-protokollaa käyttäviä ohjelmia löytyy ja on saatavissa yleisimmille käyttöjärjestelmille.

6 INTEGRAATIO

Luvussa 3 esiteltyjen laitteiden integraation toteutus ja toiminta esitetään tässä luvussa neljässä osassa, joissa kussakin tarkastellaan kahta laitetta kerrallaan. Lopputulos ei integraation osalta ole täysin full mesh -tyyppinen, eli suoraa fyysistä järjestelmän kaikkien osien välillä ei ole. Tämän työn kannalta se tarkoittaa, että kaikki SIP-signalointi GSM-VOIP-yhdyskäytävän ja IP-verkon välillä kulkee Trixboxin kautta. Sillä ei kuitenkaan ole Trixboxin kuormituksen kannalta merkitystä, sillä MV-372-yhdyskäytävä tukee vain kahta puhelinjaa.

Kuva 10 esittää laitteiden sijainnin toisiinsa nähden koulun verkossa. Palvelimilla on kiinteät IP-osoitteet eikä niiden sijaintia verkossa ole tarkoitus muuttaa. Puhelimia sen sijaan voidaan liikutella verkoissa vapaammin, sillä ne löytävät asetuksiin määritellyn VoIP-palvelimen sisä- ja ulkoverkkojen yli. UC520 oli ainut palvelin, johon puhelimet kytkettiin suoraan. Kuvassa puhelimien alla näkyvät myös numeroavaruudet. Signalointiprotokollana käytettiin yksinomaan SIP-protokollaa ja äänikoodekkina toimi G.711 alaw/ulaw.



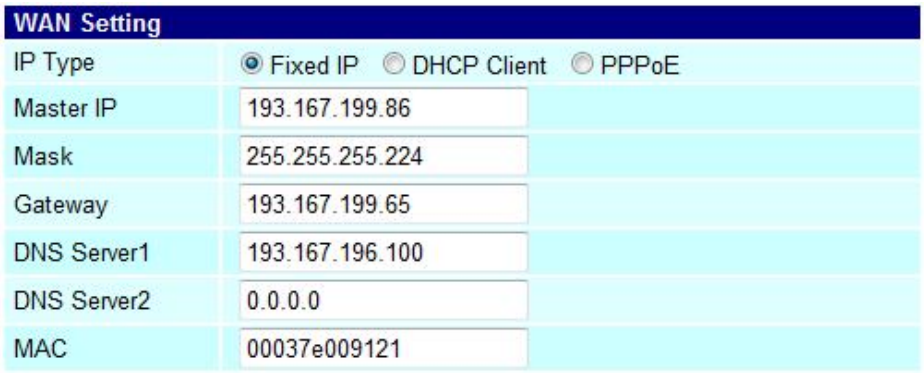
Kuva 10. VoIP-järjestelmä koulun verkossa

6.1 MV-372 ja Trixbox

Ensimmäisen työvaiheen lopullinen tavoite oli mahdollistaa puheluiden reititys gsm-puhelimen ja IP-puhelimen välillä kulkien yhdyskäytävän ja Trixbox-VoIP-palvelimen kautta. Mobiiliverkosta yhdyskäytävälle soitettaessa puhelun tulisi olla kaksivaiheinen ja mobiiliverkkoon soitettaessa yksivaiheinen. Tavoitteeseen päästiin seuraavien työvaiheiden jälkeen.

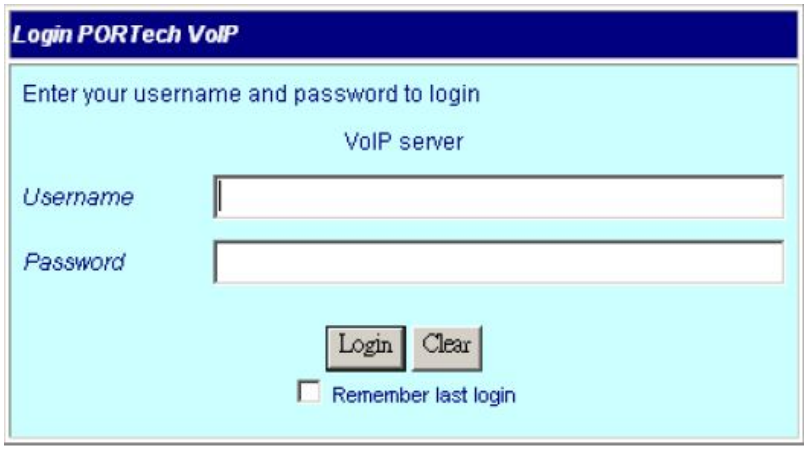
6.1.1 Portech MV-372-yhdyskäytävä

Laitteen tehdasasetusten mukaisen ip-osoitteen (192.168.0.100/32) verkko-osoite (192.168.0.0/32) ei vastannut laitteelle aiottua kohdeverkkoa. Siitä syystä laite oli kytkettävä aluksi suoraan siihen tietokoneeseen, jolla alkukonfigurointi ja päivitys tehtiin. Laite kytkettiin verkkoon WAN-portista, joten sen osoite oli muutettava kohdeverkkoon sopivaksi. Pakollisia asetuksia olivat kiinteä IP-osoite (Fixed IP), verkkomaski ja yhdyskäytävän osoite. Yhdyskäytävällä tarkoitetaan GSM-VOIP-yhdyskäytävän näkökulmasta reititintä, jolle kaikki vieraaseen verkkoon menevä liikenne ohjataan. DNS-palvelimen osoite laitettiin myös asetuksiin tulevaisuuden varalle (Kuva 11).



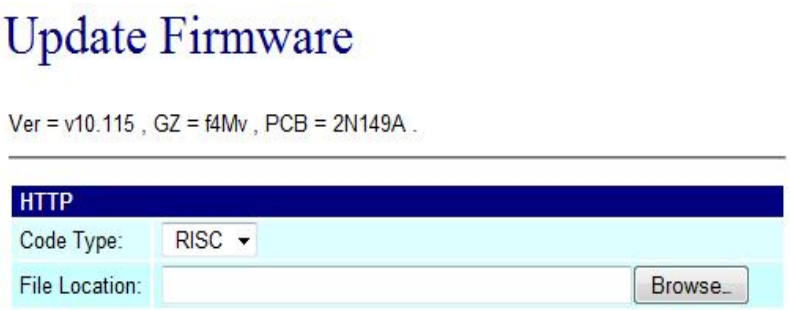
Kuva 11. WAN-portin asetukset

Sisään kirjauduttaessa käyttäjältä kysytään tunnuksia, joilla päästään laitteen asetuksiin. Osana tietoturvaa laitteen käyttäjätunnus ja salasana vaihdettiin, ennen kuin laite sijoitettiin sen varsinaiselle paikalle koulun verkkoon (Kuva 12).



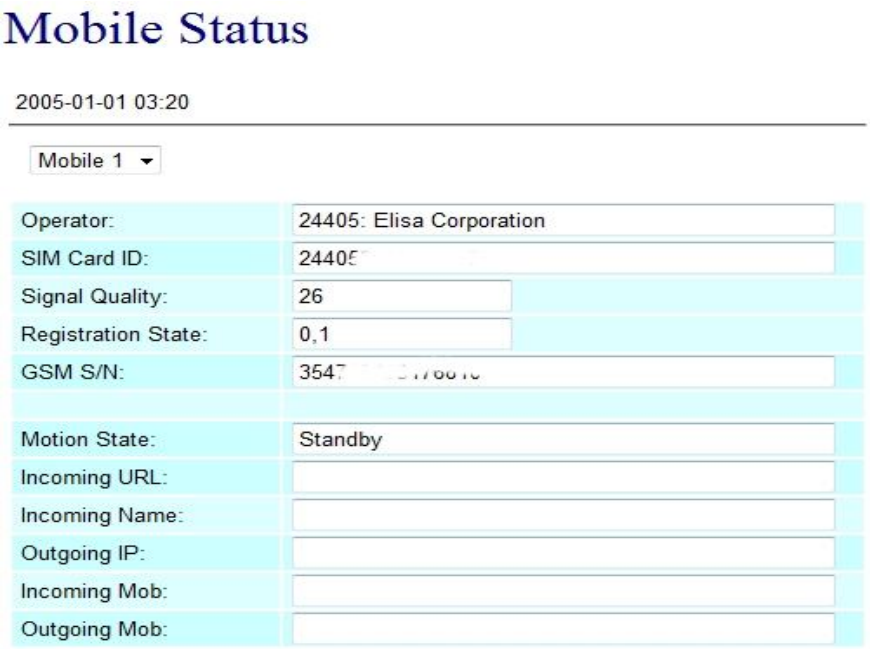
Kuva 12. Kirjautuminen gsm-VoIP-yhdyskäytävään

Aluksi haluttiin varmistaa, että laitteen sisäinen ohjelmisto on ajan tasalla, joten siihen asennettiin ohjelmiston uusin versio valmistajan web-sivuilta osoitteesta http://www.portech.com.tw/p3-HowtoupdateMV-370c.asp. Tarkoituksena oli minimoida mahdollisten ”bugien” eli ohjelmistovirheiden tai -puutteiden esiintymistodennäköisyys. Kuvasta 13 näkyy kolme päivittämisen kannalta olennaista asiaa: laitteen ohjelmistoversio (v10.115), pakatun päivitystiedoston (GZ) tunnus ja piirilevyn mallinumero(PCB). Ohjelmistoversionumerosta näkee, kuinka uusi ohjelmisto on käytössä ja kaksi muuta tunnusta auttavat oikean tiedoston valinnassa Portechin sivuilta. Koodin tyyppinä on risc, mistä voidaan päätellä, että laitteessa on risc-arkkitehtuurin mukainen prosessori. Tiedosto annetaan laiteelle pakattuna gz-tiedostona. Gz on tiedostopääte jota GNU:n kehittämä avoimen lähdekoodin gzip-ohjelma käyttää.



Kuva 13. Laitteen ohjelmiston päivitys

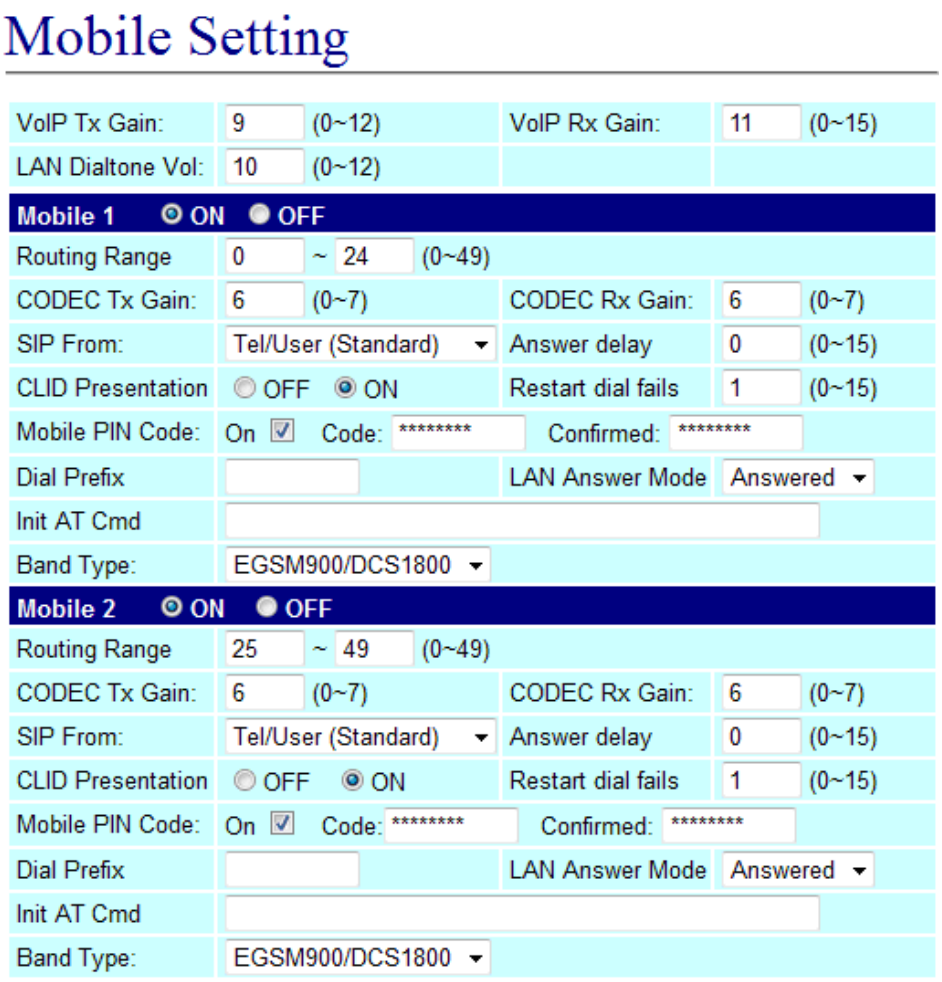
Päivityksen jälkeen laitteen tehdasasetukset palautettiin ja kaksi sim-korttia asetettiin paikoilleen. Sim-korttien pin-koodit piti syöttää laitteen matkapuhelin-asetuksiin, jotta ne rekisteröityivät verkkoon. Rekisteröitymisen onnistuminen todettiin Mobile Status –valikosta (Kuva 14).



Kuva 14. Sim-kortin tiedot onnistuneen rekisteröinnin jälkeen

Yhdyskäytävän matkapuhelinverkko-asetuksista kohdasta ”SIP From:” valittiin lähetysmuoto ”Tel/User”. Tämä asetus mahdollistaa soittajan gsm-numeron välittämisen SIP-viestissä sellaiselle VoIP-palvelimelle, johon yhdyskäytävä on rekisteröitynyt. Numeron kulku palvelimelta eteenpäin toiseen puhelimeen riippuu palvelimen asetuksista, jotka käsitellään myöhemmin.

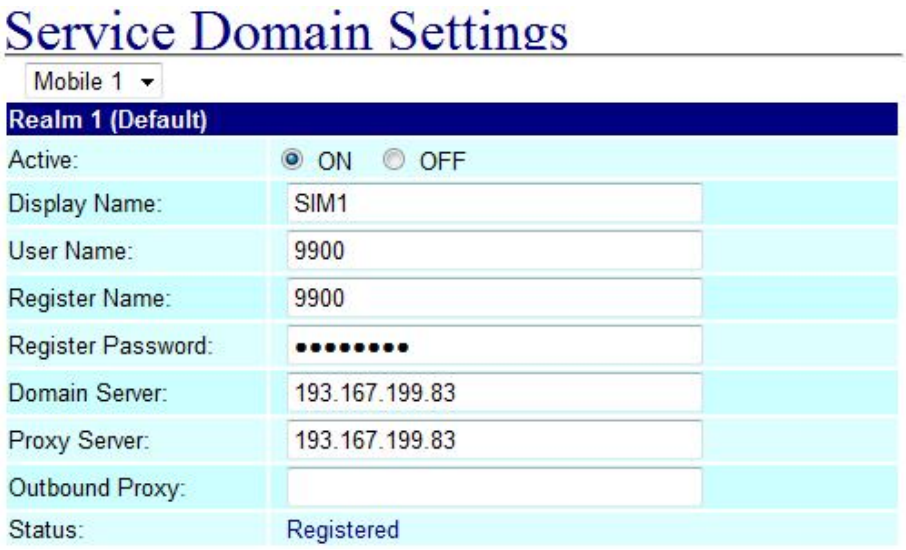
Äänenvoimakkuuden vahvistusta sekä matkapuhelinverkkoon (Rx Gain) että ip-verkkoon (Tx Gain) oli myös mahdollista muuttaa, mutta tehtyjen puhelutestien perusteella se ei ollut tarpeellista.



Kuva 15. GSM-asetukset

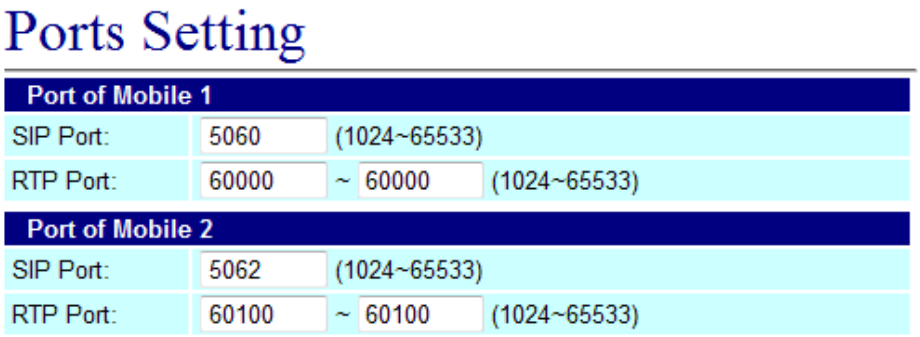
GSM-VoIP-gateway asetettiin rekisteröitymään VoIP-palvelimeen, jotta voitaisiin varmistua rekisteröinnin toimivuudesta ja toisaalta, koska laite tukee sitä. Ominaisuus myös lisää tietoturvaa, kun puhelu tulee rekisteröidyn laitteen kautta. Koska GSM-verkosta yhdyskäytävän kautta soittava puhelin ei voi rekisteröityä VOIP-palvelimeen, voidaan rekisteröinti hoitaa yhdyskäytävästä.

Yhdyskäytävä asetettiin rekisteröityyn tilaan Trixboxin kanssa määrittelemällä molemmille sim-korteille tunnukset ja palvelimen ip-osoite (Kuva 16). Rekisteröintipalvelin/rekisterinpitäjä- ja välityspalvelin ovat tässä työssä VoIP-palvelimiin integroituja ominaisuuksia, joten niiden ip-osoitteet ovat myös samat.



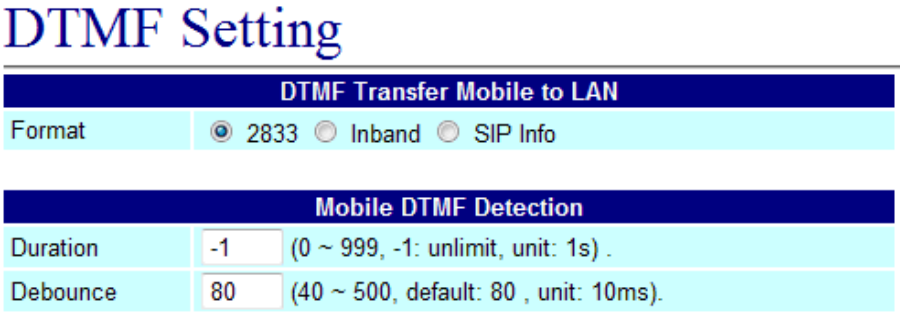
Kuva 16. Yhdyskäytävän rekisteröitymisasetukset

Kahta samanaikaista yhteyttä tukevalle yhdyskäytävälle piti määritellä molemmille yhteyksille omat udp-porttinumerot SIP- ja RTP-protokollia varten. Sim1:n SIP:lle annettiin oletus UDP-portti 5060 ja sim2:lle 5062. RTP:lle annettiin vastaavasti UDP-portit 60000 sim1:lle ja 60100 sim2:lle (Kuva 17).



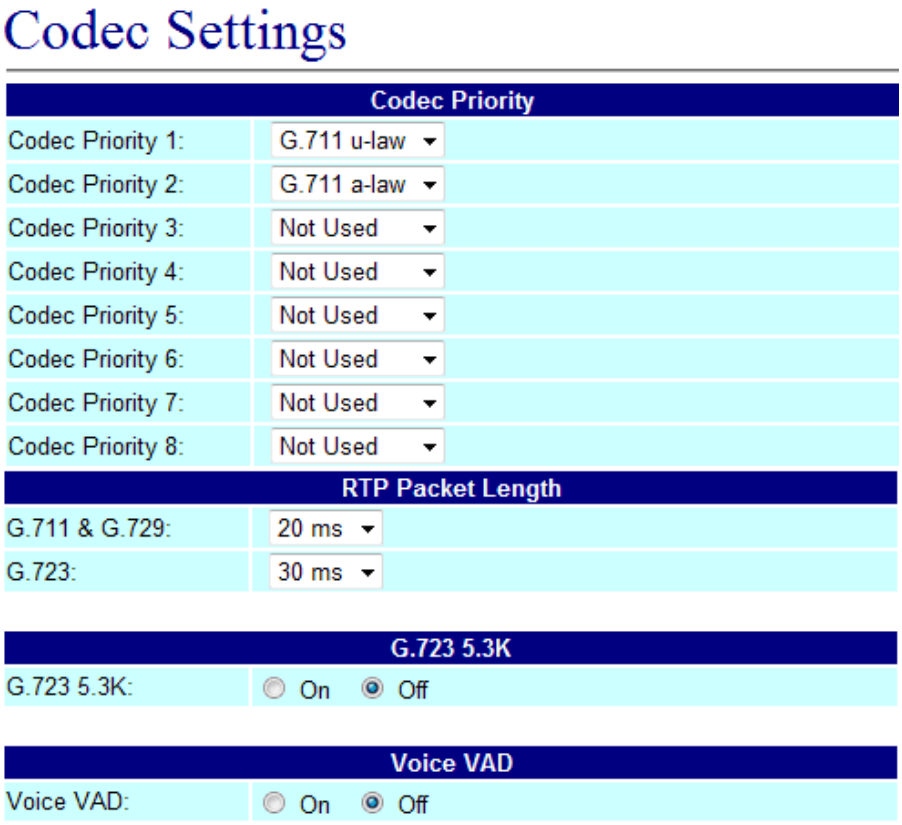
Kuva 17. Porttiasetukset

Äänitaajuusvalinnan eli DTMF:n toiminnalla on tässä työssä merkitystä soitettaessa matkapuhelimesta MV-372-yhdyskäytävän kautta VoIP-palvelimelle. Kun soittaja näppäilee järjestelmän alanumeron, lähetetään näppäillyt numerot yhdyskäytävälle kahden eri taajuisen äänen yhdessä muodostamalla äänitaajuuskoodilla. DTMF-signaalien kuljetustavaksi IP-verkossa valittiin IETF:n RFC 2833 –standardi, joka kuljettaa signaalit RTP-median mukana. Viiveitä ei muuteltu, koska äänitaajuusvalinnan tunnistus toimi perusasetuksillakin riittävän luotettavasti (Kuva 18).



Kuva 18. Dual-Tone Multi-Frequency-äänitaajuusvalinta

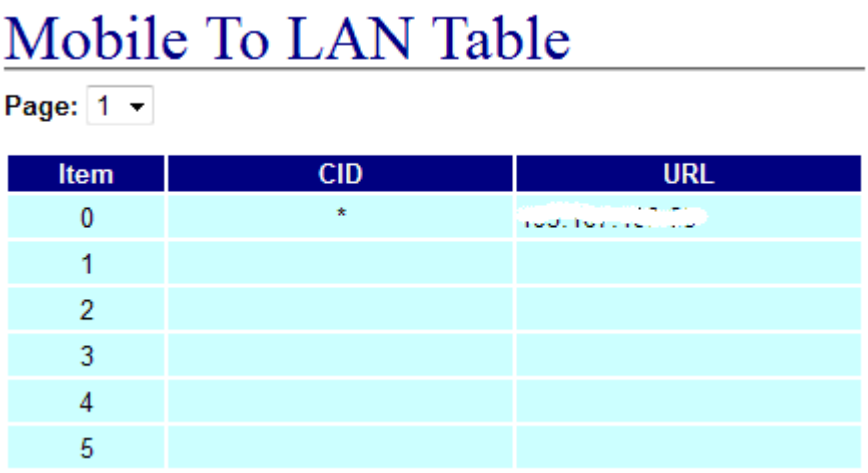
Äänikoodekkina tässä työssä pyrittiin käyttämään ensisijaisesti G.711:tä, joten sen molemmat versiot, u-law ja a-law, valittiin käyttöön. Muita koodekkeja ei niiden suuremman häviöllisyyden takia haluttu mukaan. RTP-paketteihin kuuluvan puhenäytteen pituutta ei muutettu, eikä äänen aktiviteetin tunnistusta (VAD) otettu säästämään kaistaa (Kuva 19).



Kuva 19. Puhekoodekit

Matkapuhelinverkon ja ip-verkon välisen liikenteen reititykseen on kummallekin suunnalle oma reititystaulunsa. Puheluiden reititystä varten reititystaulut jaettiin kahden sim-kortin kesken, jolloin kummallekin riittää 25 reitityssääntöä. Sim-1 käyttää taulukoiden rivejä 0-24 ja sim-2 rivejä 25-49 (Kuva 15).

Matkapuhelinverkko -> ip-verkko -suuntaiseen reititystauluun laitettiin soittajan tunnus CID-sarakkeeseen tähtimerkki (*), mikä sallii soittamisen mistä tahansa numerosta. Rivillä 0 sääntö koskee vain sim1-korttia, joten riville 25, mistä alkaa sim2-kortin osuus reititystaulusta, laitettiin sama sääntö. URL-kenttään laitettiin Trixboxin ip-osoite (Kuva 20). Verkkotunnuksen käyttö on myös mahdollista, mikäli laitteen asetuksiin on laitettu toimivan DNS-palvelimen osoite .



Kuva 20. Matkapuhelinverkko -> ip-verkko -reititystaulu

IP-verkosta matkapuhelinverkkoon reitittämistä varten muokattiin toista reititystaulua. URL-sarakkeeseen laitettiin tähti, jolloin mikä tahansa ip-osoite kelpaa. Tähti oltaisiin myös voitu korvata Trixboxin ip-osoitteella ja dns-nimellä, koska kaikki puhelut ip-verkosta mv-372-yhdyskäytävälle tulevat sen kautta. Call Num eli puhelinnumero, johon puhelu ohjataan, määritettiin risuaita-merkillä (#). Silloin yhdyskäytävä ohjaa puhelun palvelimelta tulevassa sip-viestissä olevaan kohdenumeroon. Kuvassa 21 rivillä 25 näkyvä sääntö koskee sim2:sta.

Item	URL	Call Num
20		
21		
22		
23		
24		
25	*	#

Kuva 21. IP-verkko -> matkapuhelinverkko -reititystaulu

6.1.2 *Trixbox-VoIP-palvelimen asetukset*

Trixbox oli valmiiksi asennettu koulun verkkoon, kun tätä työtä lähdettiin tekemään. Koska gsm-VoIP-yhdyskäytävä asennettiin samaan verkkoon Trixboxin kanssa, oli verkkoyhteys näiden laitteiden välillä kunnossa. Trixboxin konfigurointi suoritettiin kokonaan http-yhteydellä web-pohjaisen hallintasivuston kautta. Asteriskin osalta konfiguroinnin voi suorittaa myös konfiguraatiotiedostoja muokkaamalla, mutta esimerkiksi extension.conf-tiedostossa oli alussa varoitus, jossa kehoitettiin välttämään tiedoston editoimista ja kerrottiin FreePBX:n tekevän sen automaattisesti.

Aluksi Trixboxin moduulit sekä alustana toimiva Cent Os -käyttöjärjestelmä haluttiin päivittää. Cent Os:n Bash-komentotulkkiin otettiin yhteys ssh:lla ja suoritettiin päivityksien tarkistus ja asennus käyttämällä Yum-pakettienhallintaohjelmaa.

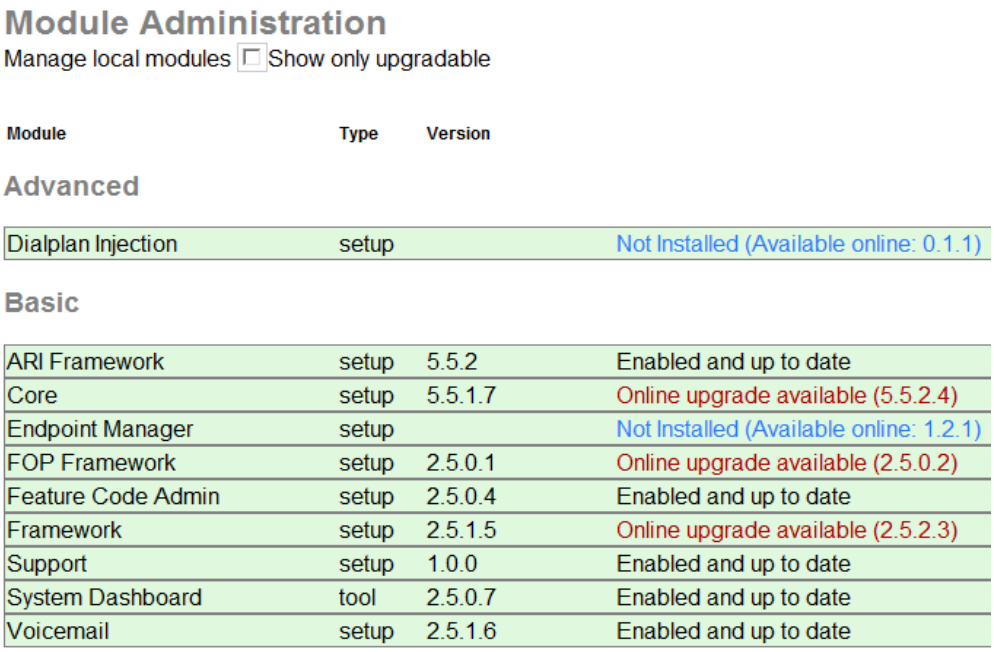
- päivitysten tarkastuskomento – yum check-update
- päivitysten asennuskomento – yum update.

Cent Os -päivityksien jälkeen oli vuorossa Trixboxin ohjelmistomoduulien päivitykset ja mahdollisten lisämoduulien asennus. Moduulien päivityksien tarkastaminen käy kaikki kerralla -periaatteella, jonka tuloksena nähdään kaikki saatavilla olevat päivitykset ja ladatut mutta asentamattomat moduulit. Myös saatavissa olevat ohjelmistopaketit tarkistettiin uusien hyödyllisten ominaisuuksien toivossa. Sekä moduulien että ohjelmistopakettien tarkistus, lataaminen ja asennus tapahtuu Trixboxin hallintasivujen kautta helposti.

610	trixbox	atl1	atl1 kernel modile	1.2.40.2-1	☐	No Update	Not Installed
611	trixbox	ez-ipupdate	Client for Dynamic DNS Services	3.0.11b8-3	☐	No Update	Not Installed
612	trixbox	fftw	Fast Fourier Transform library	3.1.2-3	☐	No Update	Not Installed
613	trixbox	firmware-linksys	Firmware for Linksys phones	5.1.7-1	☑	No Update	Not Installed
614	trixbox	firmware-polycom	Firmware for Polycom phones	3.0.1-2	☐	No Update	Not Installed
615	trixbox	flite-devel	Development files for flite	1.3-9	☐	No Update	Not Installed

Kuva 22. Trixboxin ohjelmistopaketit

Kuvassa 22 näkyy valittuna oleva ohjelmistopaketti, joka sisältää Linksys-merkkisten puhelinten ohjelmistopäivityspaketin. Tällainen paketti mahdollistaa kyseisen valmistajan IP-puhelinten ohjelmistopäivityksen suoraan VoIP-palvelimelta. Koska koululla on myös yksi tai useampia Linksys-merkkisiä puhelimia, päätettiin päivityspaketti asentaa. Trixboxille ladattiin myös toinen ohjelmistopaketti nimeltään Endpoint Manager, josta kerron myöhemmin.



Module Administration

Manage local modules ☐ Show only upgradable

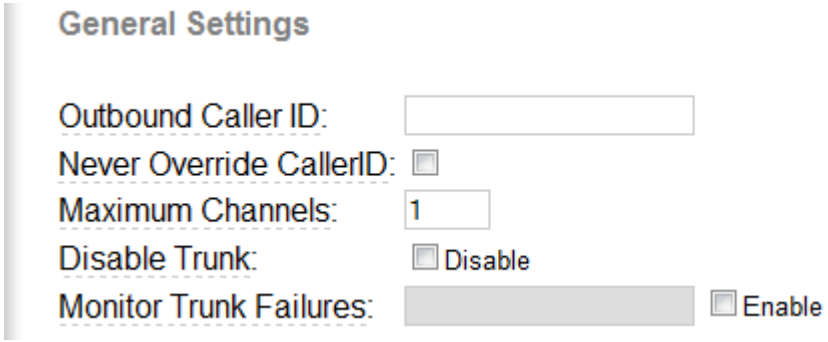
Module	Type	Version	
Advanced			
Dialplan Injection	setup		Not Installed (Available online: 0.1.1)
Basic			
ARI Framework	setup	5.5.2	Enabled and up to date
Core	setup	5.5.1.7	Online upgrade available (5.5.2.4)
Endpoint Manager	setup		Not Installed (Available online: 1.2.1)
FOP Framework	setup	2.5.0.1	Online upgrade available (2.5.0.2)
Feature Code Admin	setup	2.5.0.4	Enabled and up to date
Framework	setup	2.5.1.5	Online upgrade available (2.5.2.3)
Support	setup	1.0.0	Enabled and up to date
System Dashboard	tool	2.5.0.7	Enabled and up to date
Voicemail	setup	2.5.1.6	Enabled and up to date

Kuva 23. Trixboxin moduuleita (kuvassa vain osa)

Kuvassa 23 näkyvä Endpoint Manager -moduuli sekä kaikille muille moduuleille löytyneet päivitykset asennettiin. Asennetut ja päivitetyt moduulit olivat kooltaan vain muutamasta sadasta kilotavusta muutamaan megatavuun, eikä niiden asentamiseen kulunut kuin muutama minuutti. Pienistä palasista koostuvan järjestelmän päivitys on nopeaa, eikä aina vaadi uudelleen käynnistystä ja siitä aiheutuvaa käyttökatkoa.

Seuraavaksi konfiguroitiin sip.conf-tiedostoa web-hallintasivujen avulla. GSM-VOIP-yhdyskäytävän ja Trixboxin välistä SIP-signalointia ja rekisteröitymistä varten luotiin kummallekin SIM-kortille oma SIP-trunk-linkki. Kanavien maksimimäärä linkkien sisällä rajoitettiin yhteen, jotta palvelin lopettaisi mahdollisen uuden kutsun linjan ollessa varattuna.

Kuvasta 24 nähdään trunk-linkin yleiset asetukset SIM2-lle. Outbound Caller ID, eli soittavan osapuolen tunnus tai numero voidaan haluttaessa määritellä uudestaan, kun puhelu kulkee trunk-linkin kautta. GSM-verkkoon soitettaessa siitä ei kuitenkaan ole hyötyä, koska vastaajalle lähetettävä soittajan numero on aina sen sim-kortin numero, jota yhdyskäytävä käyttää.



Kuva 24. Yleiset SIP-asetukset sim2

Sip-yhteysasetukset on jaettu kahteen osaan, saapuvien ja lähtevien mukaan. Trixboxin ja GSM-yhdyskäytävän väliseen sip-liikenteeseen laitettiin minimaaliset asetukset, joilla yhteys saatiin toimimaan. Työn edetessä määriteltiin enemmän yhteysasetuksia muille SIP-TRUNK-linkeille. Asetukset kuuluvat Trixboxin Asterisk-puhelinvaihdeohjelmaan. Asterisk määrittelee suhteensa muihin sip-laitteisiin kolmen SIP-oliotyypin avulla:

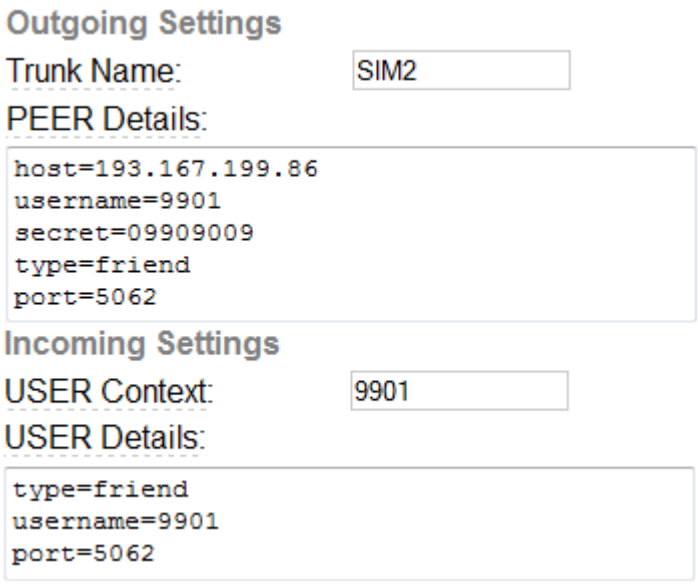
- PEER on olio, jolle Asterisk lähettää puheluita.
- USER on olio, jolta saapuvat puhelut Asterisk lähettää eteenpäin.
- FRIEND olio on kahden edellisen yhdistelmä, joten useimmat puhelimet ovat FRIEND-olioita.

Lähtevien puheluiden SIP-yhteysasetukset koostuvat komento-parametri –pareista. Sim2:n yhteysasetuksiin laitettiin seuraavat komennot (Kuva 25):

- HOST: Trixboxin IP-osoite
- USERNAME: käyttäjänimi SIM2:lle.
- SECRET: salasana SIM2:lle
- TYPE: oliotyyppi
- PORT: UDP-portti SIP-protokollalle

Koska IP-OSOITE on molempien SIM-korttien osalta sama, piti porttinumero muuttaa toiselle SIM-kortille myös Trixboxin asetuksista. Molemmilla SIM-korteilla on myös oma käyttäjänimi ja salasana. Oliotyypiksi valittiin friend, koska SIP-merkinantoliikenne voi kulkea kumpaan suuntaan tahansa.

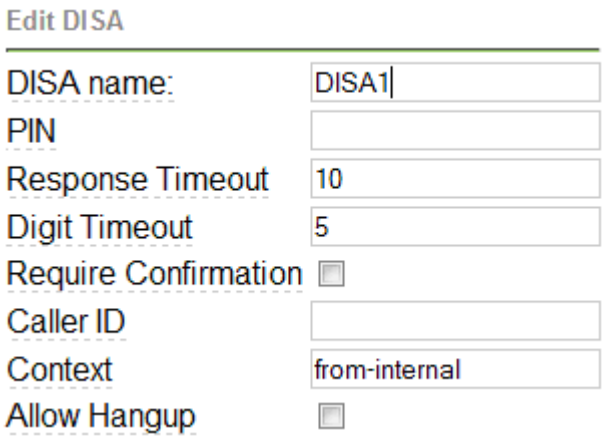
Asteriskin puhelunohjaus perustuu osittain kontekstien käyttämiseen. Kontekstit luovat vaikutusalueita lajittelemalla alanumeroita ja kanavia. Jokainen konteksti sisältää yhden tai useamman alanumeron, osoitteen tai viittauksen toiseen kontekstiin. Kontekstit sijaitsevat extensions.conf-tiedostossa ja niihin viitataan monissa muissa konfiguraatiotiedostoissa. Kontekstiksi (User context) SIM1:lle laitettiin sen käyttäjätunnus (Kuva 25).



Kuva 25. Sip-yhteysasetukset sim2 2/2

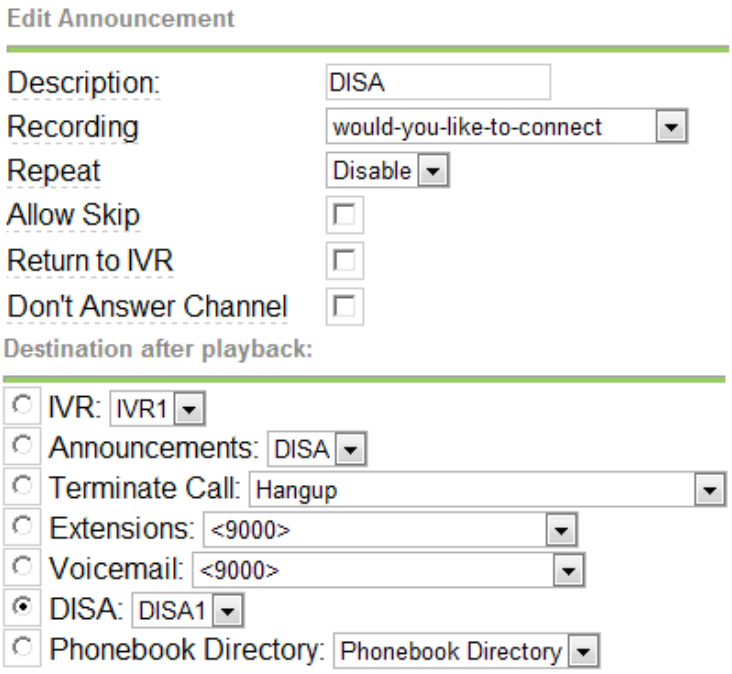
Trixbox ei voi reitittää saapuvaa puhelua mihinkään numeroon, jos sitä ei ole annettu. Tällainen tilanne toteutuu soitettaessa mobiiliverkosta GSM-VOIP-yhdyskäytävään, josta puhelu ohjautuu suoraan Trixboxiin. Soittajan täytyy voida valita myös alinumero, johon soittaa. Puhelun soittamisesta tulee kaksivaiheinen.

Mobiiliverkosta yhdyskäytävään soitettujen puheluiden kaksivaiheisuus toteutettiin Trixboxin DISA (Direct Inward System Access) -moduulin avulla. Tarkoituksena on tehdä puhelusta kaksivaiheinen ja antaa soittajalle mahdollisuus soittaa mihin tahansa numeroon, johon Trixbox voi puhelun reitittää. DISA tarjoaa myös joitakin lisäominaisuuksia, kuten salasanan kyselyn tai soittavan osapuolen numeron vaihtamisen toiseksi ennalta määritetyksi numeroksi. Myös kontekstin voi muuttaa DISA:n kautta soitettaessa. Oletusarvona on ”from-internal”, jolloin Trixbox sallii puhelun reitittämisen kaikkiin paikallisiin numeroihin sekä lähteviin reitteihin (Kuva 26).



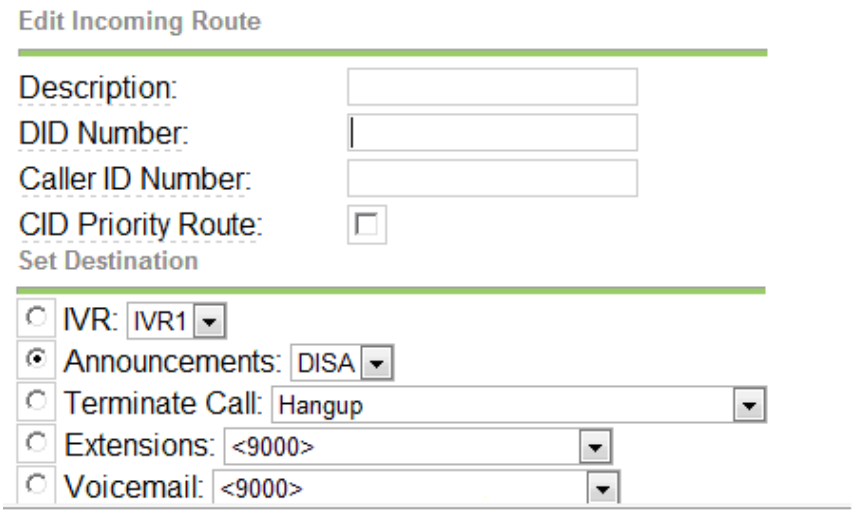
Kuva 26. Disa (Direct Inward System Access)

Tehdyissä kokeissa huomattiin, että Disa tarjoaa soittajalle vain lyhyen merkkiäänen, joka koettiin huonoksi tavaksi informoida soittajaa syöttämään alanumero. Ratkaisuna siihen oli tiedotus (announcement) -moduuli, joka ottaisi puhelut vastaan ennen DISAa. Tiedote mahdollistaa informatiivisemmat äänitteet sekä muita lisäominaisuuksia, kuten tiedotteen toistamisen ja omien WAW-äänitiedostojen käyttämisen. Tiedotteelle annettiin nimeksi Disa ja äänitteeksi valittiin oletusäänite (Kuva 27).



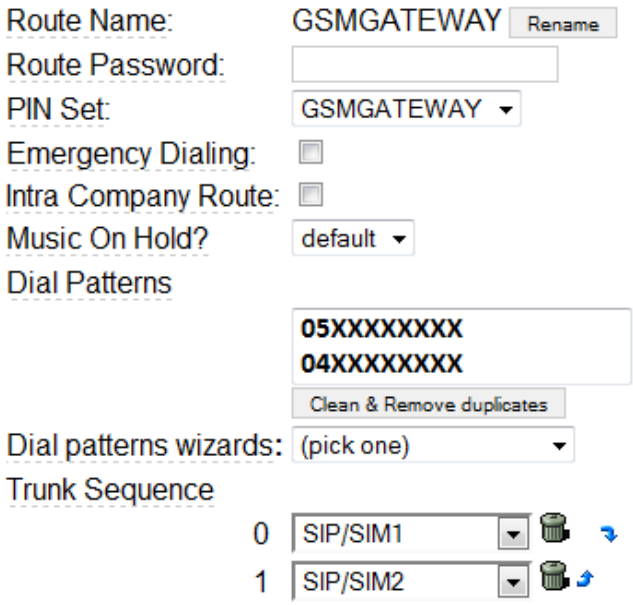
Kuva 27. Tiedote-moduuli ohjaa DISAan

Jotta Trixbox ohjaisi sekä GSM-VOIP-yhdyskäytävän kautta tulevat että mahdolliset muut epäselvät puhelut tiedote-moduuliin, tehtiin saapuva reitti (incoming route), jossa ei ole määritelty soittajan numeroa (Caller ID Number) (Kuva 28). Silloin Trixbox ohjaa puhelun kyseiseen reittiin, vaikka sitä ei olisi sisällytetty numeroanalyyseihin. Kuten kuvasta 21 näkyy, reitti osoitettiin tiedote-moduuliin nimeltä Disa. Reitin voi ohjata myös yksittäiseen numeroon, ääniviestiin, IVR:lle (Interactive Voice Response) tai se voi päättää puhelun.



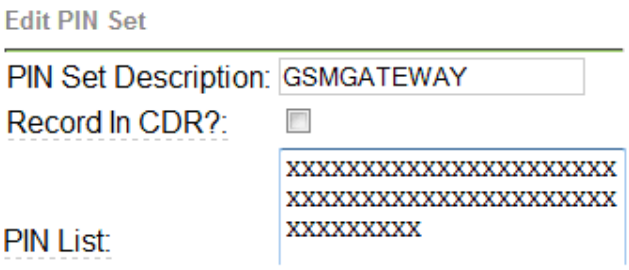
Kuva 28. Reitti ohjaa tiedotteeseen.

Puheluiden reititys Trixboxista GSM-VOIP-yhdyskäytävälle toteutettiin lähtevällä reitillä, johon ohjataan GSM-verkkoon tarkoitetut puhelut. Reitin asetuksia muokattiin määrittelemällä kaksi numerokaavaa (Dial Patterns), joiden perusteella Trixbox valitsee kyseisen reitin (Kuva 29). Kaavat perustuvat siihen tietoon, että suomalaiset matkapuhelinnumerot ovat joko 04- tai 05-alkuisia ja 10 numeron mittaisia [4]. Reitti asetettiin kulkemaan ensisijaisesti SIP-trunk-linkin SIM1 kautta, mutta sen ollessa varattuna ohjautuu reitti SIM2:lle.



Kuva 29. GSM-yhdyskäytävälle lähtevän reitin asetukset

Reitti GSM-verkkoon haluttiin suojata luvattomalta käytöltä. Se toteutettiin asettamalla reitille PIN-tunnus. PIN-tunnuksen luominen tapahtuu oman moduulinsa avulla, joka mahdollistaa useammankin tunnuksen luomisen. Tapahtumat voidaan myös kirjata puhelurekisteriin (Call Data Record), joka sijaitsee __/var/log/asterisk/cdr-csv –hakemistossa. Rekistereitä on useita, mutta Master.csv-tiedosto sisältää kaikki rekisterit. (Kuva 30)



Kuva 30. PIN-tunnusten moduuli

6.2 Trixbox ja Call Manager

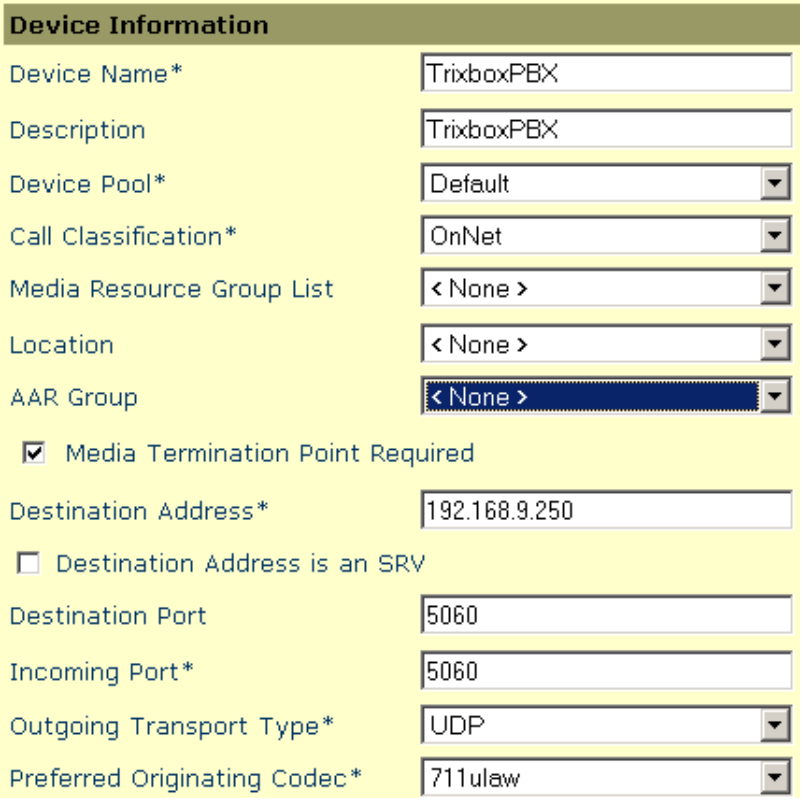
Tämän työvaiheen tarkoitus oli sovittaa SIP-merkinanto ja puheluiden reititys Cisco Call Managerin ja Trixboxin välillä. Se mahdollistaa puhelun kahden puhelimen välillä, joista toinen on rekisteröitynyt Trixboxiin ja toinen Call Manageriin. Toiminnan olisi oltava yksivaiheista, eli soittavan osapuolen ei tarvitsisi näppäillä kuin yksi numero. Tavoitteeseen päästiin seuraavien työvaiheiden jälkeen.

6.2.1 Cisco Call Manager

Call Managerin konfigurointi tapahtui Trixboxin tapaan web-pohjaisen hallintapaneelin avulla. Aluksi konfiguroitiin SIP-trunk-asetukset Call Manageriin. SIP-signaloinnin toimivuuden kannalta tärkeimmät asetukset koskevat protokollia ja laitteiden yksilöllisiä tietoja (Kuva 31), joita ovat:

- Device Name: yksilöllinen nimi
- Device Pool: mikäli käytetään useampaa Call Manageria kuorman jakamiseksi.
- Call Classification: puheluiden luokittelu paikalliseen verkkoon kuuluvaksi tai kuulumattomaksi.
- Destination Address: kohdelaitteen (Trixbox) ip-osoite
- Destination port: kohdelaitteen UDP-portti SIP-liikenteelle
- Incoming port: Call Managerin UDP-portti SIP-liikenteelle
- Outgoing transport type: lähtevän liikenteen kuljetusprotokolla
- Preferred originating codec: etuoikeutettu äänikoodekki.

Edellä esitettyjen asetusten on oltava oikein, jotta signalointi toimisi. Puheluiden luokittelu (Call Classification) -asetuksen ollessa ”OnNet”, mahdollistaa Call Manager ulkoverkosta tulevan puhelun ohjaamisen toiseen ulkoverkkoon [t]. UDP-porttinumeroita muutettaessa oletusasetuksesta (5060) kannattaa varmistaa, että asetukset laitteiden välillä eivät ole keskenään ristiriidassa. Äänikoodekin valinta vaikuttaa siihen, mitä koodekkia Call Manager ehdottaa käytettäväksi puhelussa, eikä se siten ole absoluuttinen. Edellä olevien asetusten lisäksi oli vielä pitkä lista muita asetuksia, jotka päätettiin jättää oletusarvoihinsa.

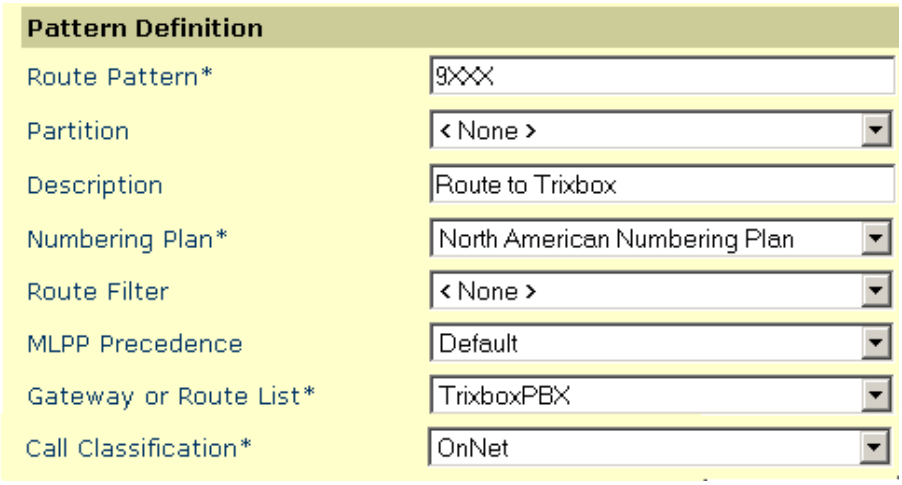


Kuva 31. SIP-trunk laitetiedot Call Managerin asetuksissa

Puheluiden ohjaaminen SIP-trunk-linkkiä pitkin Trixboxille toteutettiin numeron rakenteeseen perustuvalla reitittämisellä samalla periaatteella kuin Trixboxissa jo aiemmin tehtiin. Call Managerissa puhutaan Route Pattern -määrityksestä, jonka avulla päätetään lähtevän puhelun reitityksestä. Kuten SIP-trunkin määrityksessä, myös tässä suurin osa asetuksista sai jäädä oletusarvoihin. Kuvauksen (description) lisäksi vain pakolliset asetukset määritettiin (Kuva 32):

- Route Pattern: kuvaus numerosarjasta, joka reitittää puhelun ulos trunk-linkistä.
- Numbering Plan: numerosuunnitelma
- Gateway or route list: ulos lähtevän reitin valinta
- Call Classification: Puhelun luokittelu (katso trunk-asetukset).

Trixboxiin rekisteröidyille puhelimille annetut numerot ovat neljän numeron mittaisia ja alkavat aina numerolla 9. Kun Call Manageriin rekisteröidyllä puhelimella soitetaan tällaiseen numeroon, ohjautuu se määritelmän 9XXX mukaisesti Trixboxille. Numerosuunnitelma-asetus (Numbering plan) koskee televerkon numeroita, joita tässä työssä ei käsitellä, joten sillä ei ole merkitystä, vaikka se onkin pakollisten asetusten joukossa. Uloslähtöreitiksi valittiin jo aiemmin tehty TrixboxPBX-niminen SIP-trunk-linkki.



Kuva 32. Call Managerin route pattern -määritys

6.2.2 Trixbox

SIP-trunk-linkin asetukset Call Manageria varten tehtiin osittain samaan tapaan kuin aiemmin yhdyskäytävää varten (Kuva 33). Sekä lähtevälle että saapuvalle liikenteelle laitettiin samat asetukset. Laitteissa on kuitenkin eroavaisuuksia, jotka täytyy ottaa huomioon kaikkia asetuksia tehdessä. Call Manager ei esimerkiksi tue rekisteröitymistä trunk-linkin kautta.

Tällä kertaa trunk-linkkiin tehtiin enemmän asetuksia, joista valtaosaa ei käytetty aiemmin esitellyssä trunk-linkissä. Uusia asetuksia ovat:

- qualify: Tarkistaa yhteyden linjan toisessa päässä olevaan sip-olioon.
- nat: Menetelmä joka mahdollistaa liikenteen reitittämisen NAT-osoitemuunnoksen yli (No = ei käytössä).
- insecure: Suorittaa autentikoinnin (very = sallii rekisteröityneiden puhelinten soittaa ilman uudelleenautentikointia).
- fromdomain: Kertoo mistä toimialueesta SIP-puhelu tulee.
- dtmf: Määrittelee miten DTMF-signaalit kuljetetaan verkossa.
- disallow: Poistaa äänikoodekkeja käytöstä (all = kaikki pois käytöstä).
- allow: Ottaa äänikoodekkeja käyttöön. Esim. ”Allow = ulaw” (G.711)
- context: Määrittää asiayhteyden (katso Trixbox-VoIP-palvelimen asetukset).
- canreinvite: Määrittää INVITE-viestin uudelleenlähetyksen (no: ei uuden invite viestin lähetystä).

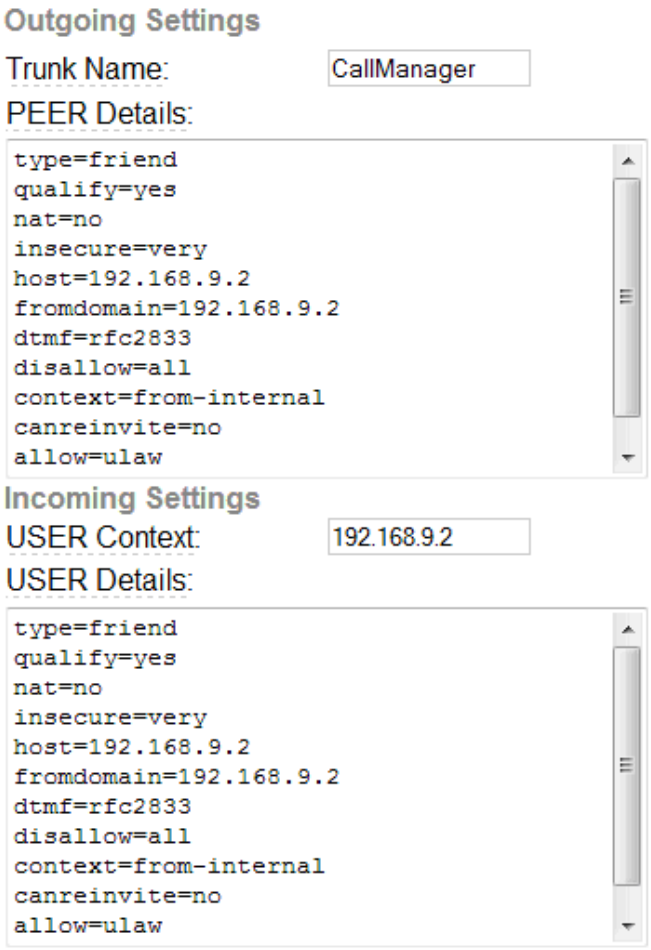
Koska Call Manager ei tue rekisteröitymistä SIP-trunk-linkin kautta, käytetään naapurilaitteen tunnistamiseen ja ominaisuuksien selvittämiseen qualify-komentoa. Jos parametriksi on annettu ”yes”, lähettää laite SIP OPTIONS –komennon 60 sekunnin välein ja odottaa vastausta 2 sekunnin kuluessa. Mikäli vastausta ei kuulu, olettaa laite naapurin olevan pois toiminnasta. SIP OPTIONS mahdollistaa naapurin ominaisuuksien selvittämisen ilman tarvetta soittaa naapurille.

Fromdomain-komennolla kerrotaan lähtevän SIP-viestin sisällä. mistä osoitteesta viesti tulee. Saapuviin viesteihin asetuksella ei ole merkitystä, vaikka se kuvassa 26 onkin saapuvien asetuksiin epähuomiossa joutunut.

INVITE-viestien uudelleen lähettäminen mahdollistaa RTP-median lähettämisen suoraan soittavien puhelimien välillä, jolloin sen ei tarvitse kiertää palvelimen kautta. Tämä tapahtuu yhteydenmuodostusdialogin aikana.

Äänikoodekeista haluttiin sallia vain G.711 alaw- ja ulaw -koodekit. Oletuksena kaikki ovat sallittuja, joten ensin oli poistettava kaikki käytöstä DISAL-

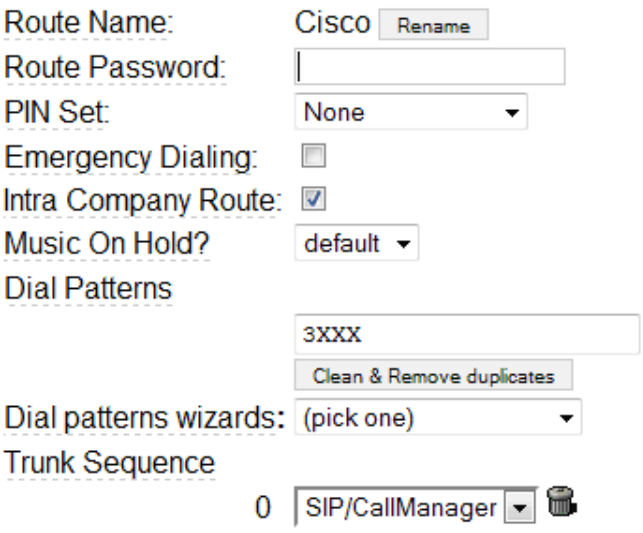
LOW-komennolla ja sen jälkeen sallittava halutut koodekit ALLOW-komennolla. Kuvassa 33 piiloon jää ”allow = alaw”-komento.



Kuva 33. SIP-trunk asetukset Trixbox - Call Manager -yhteydelle

Puheluiden ohjaamiseksi Trixboxista Call Managerille luotiin uusi lähtevä reitti (Kuva 34). Kaikki Call Manageriin rekisteröidyt puhelinnumerot ovat neljä numeroa pitkiä ja alkavat numerolla 3. Siten numerokaavaksi tähän reittiin tuli 3XXX.

”Intra Company Route” -valinta varmistaa, että alkuperäinen soittajan numero lähetetään trunk-linkin kautta. Lopuksi valitaan vielä alavetovalikosta edellisessä vaiheessa tehty trunk-linkki.



Kuva 34. Lähtevä reitti Trixbox -> Call manager

6.3 Trixbox ja UC520

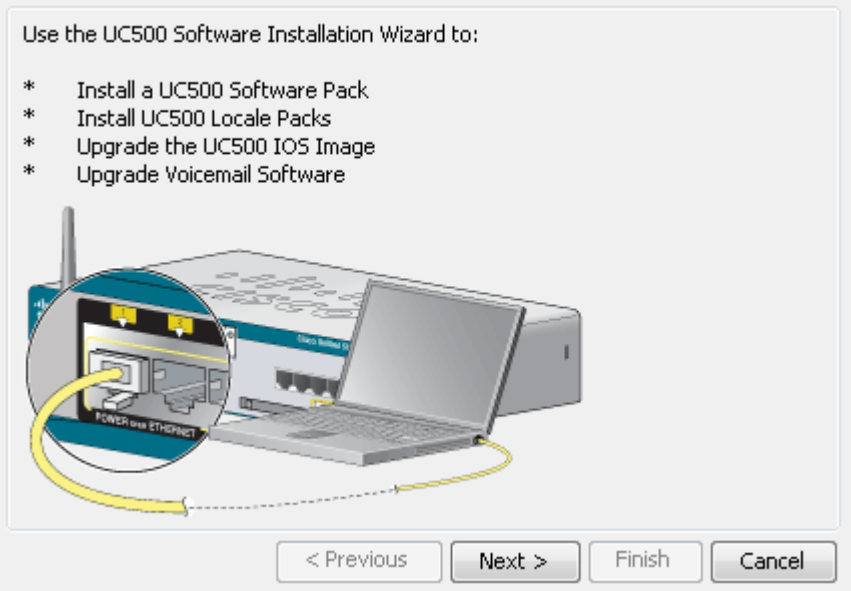
UC520:n mukaantulo lisäsi mahdollisuuden myös analogisten puhelinten ja ISDN-puhelinten liittämiseen. UC520 oli myös työn ainut laite, johon puhelimet kytkettiin suoraan. Konfigurointi sujui Trixboxin kohdalla rutiininomaisesti. UC520:n kohdalla vastaan tuli uusia haasteita, joista kuitenkin selvittiin ja jotka koettiin hyvin opettaviksi.

6.3.1 UC520

UC520:n konfigurointi yritettiin hoitaa kokonaan CCA (Cisco Configuration Assistant) -ohjelmaa käyttäen, mutta trunk-linkin asetukset konfiguroitiin lopulta CLI-komentoliittymän kautta. Tämä johtui siitä, että CCA:n kautta konfigurointi ei vaikuttanut yhtä loogiselta kuin esimerkiksi Call Managerin tapauksessa. CLI todettiin varmemmaksi ja yksinkertaisemmaksi konfigurointitavaksi sekä työn sisältöä positiivisesti monipuolistavaksi.

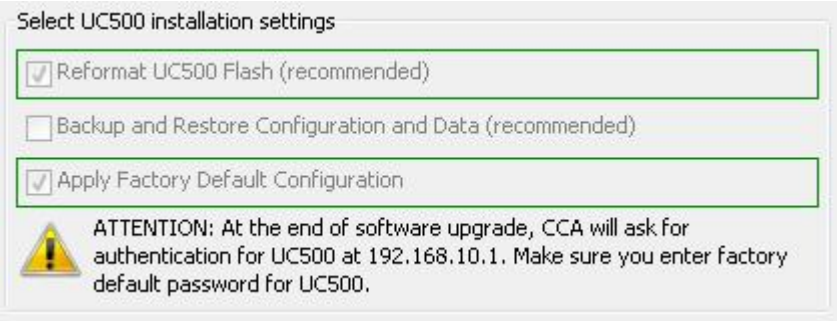
Yhteys CCA:lla otettiin yhteen UC520:n kahdeksasta LAN-portista suoraan tietokoneelta, joten tietoturva oli sen puolesta paras mahdollinen. Ennen Call Manager Expressin konfiguroimista sen ohjelmisto päätettiin päivittää CCA:n avulla (Kuva 35). UC520:n ohjelmisto on pakattu zip-tiedostoon, jonka CCA siirtää UC520:lle TFTP-tiedonsiirtoprotokollalla. TFTP:n käyttöä saattaa haitata palomuuri, joka voi estää yhteyden, tai sen voi sekoittaa toinen samanaikaisesti suoritettava tftp-ohjelma. Päivityshetkellä uusimman ohjelmisto-

pakkauksen versio oli 8.1.0. Päivitys on hyvin suoraviivaista, eikä käyttäjän tarvitse tehdä monimutkaisia valintoja päivityksen aikana. Koska konfiguroiminen haluttiin aloittaa laitteen tehdasasetuksista, ei vanhoja asetuksia otettu talteen (Kuva 36).

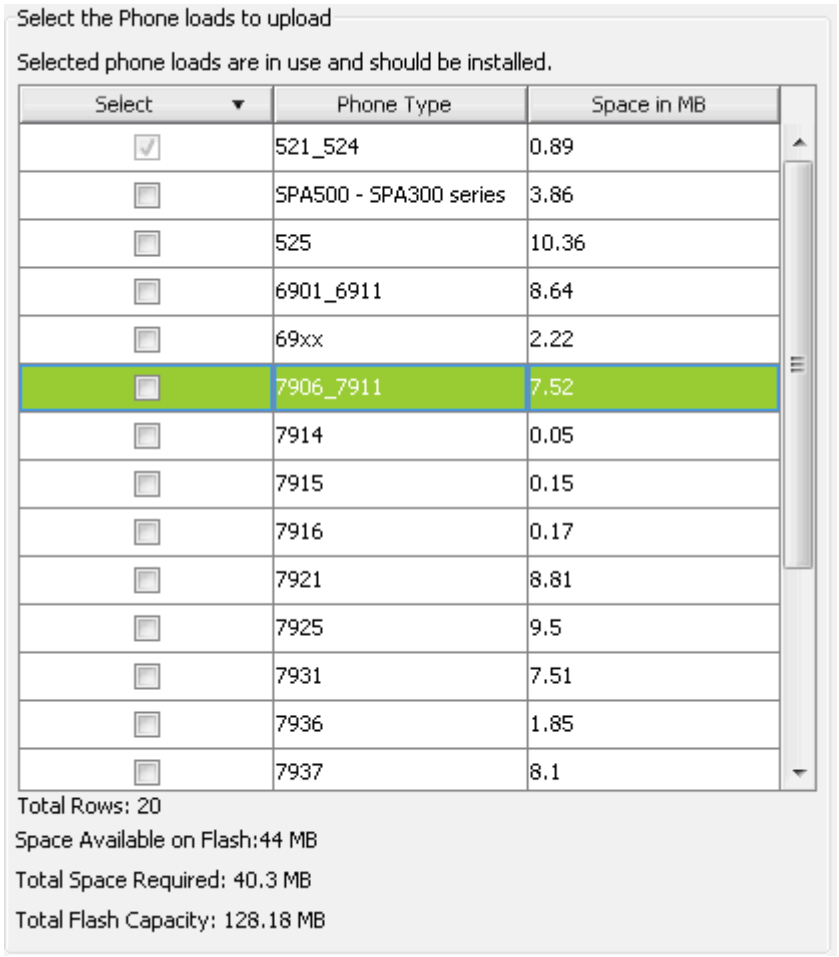


Kuva 35. UC520:n ohjelmiston päivitys

Päivityksen aikana CCA kysyy, mitä puhelinohjelmistoja asennukseen halutaan sisällyttää (Kuva 37). Koska ohjelmisto asentuu Compact Flash -muistikortille, on syytä varmistaa, että siellä on tilaa kaikelle halutulle datalle. UC520:ssä alkuperäisenä ollut 128 MB:n muistikortti oli liian pieni haluttujen puhelinohjelmistojen tallettamiseen, joten se vaihdettiin 256 MB:n muistikorttiin ja ohjelmiston asennus aloitettiin alusta uudelle kortille. Tiedostojärjestelmän tulee olla tyypiltään FAT, jotta UC520 voi käynnistyessään löytää ja ladata IOS-tiedoston muistikortilta.



Kuva 36. UC500-ohjelmiston asennusasetukset



Kuva 37. puhelinohjelmistojen valinta asennuksen yhteydessä

SIP-trunk-linkki konfiguroitiin ottamalla yhteys Putty-asiakasohjelmalla UC520:n komentoliittymään (CLI). Käytännössä yhteys UC520:n konsoliporttiin otettiin suoraan PC-tietokoneelta, joten yhteyden turvallisuudesta ei tarvinnut huolehtia.

Oletusasetuksilla UC520 kysyy käyttäjänimeä ja salasanaa kirjautumistavasta riippumatta. Konfigurointi voidaan aloittaa ns. privileged-moodista, joka on yksi Ciscon laitteiden IOS-konfigurointimoodeista. Privileged-moodiin siirryttäessä salasanaa kysytään uudestaan. Konfiguroinnit näkyvät esimerkissä 1.

dial-peer voice 100 VoIP ; Määrittelee yhteyden yksilöivän numeron ja yhteystavan (VoIP).

description TO TRIXBOX ; Kuvaa yhteyden nimen.

destination-pattern 9… ; Määrittelee koodin jota soitetun numeron tulee vastata.

session protocol sipv2 ; Määrittelee merkinantoprotokollan.

session target ipv4: 193.167.199.83 ; Määrittelee kohdeosoitteen.

dtmf-relay rtp-nte ; Määrittelee DTMF-signaalien kuljetustavan.

codec g711alaw ; Määrittelee käytettävän puhekoodekin.

no vad ; Ottaa puheen aktiivisuuden tunnistuksen pois päältä.

Esimerkki 1. UC520:n sip-yhteysasetukset Trixboxille.

Puhelut GSM-numeroihin ohjattiin myös Trixboxin kautta koodilla 0....., jossa pisteet edustavat mitä tahansa merkkiä. Ensimmäiset soittoyritykset kumpaankin suuntaan sekä Trixboxille että Call Managerille kuitenkin epäonnistuivat. Asiaa tutkittiin UC520:n komentoliittymän kautta ja huomattiin, että pääsylistoilla toteutetun palomuurin lista 104 estää saapuvan liikenteen kyseisiltä palvelimilta. Konfiguraatioita tutkimalla huomattiin, että lista oli osoitettu suodattamaan UC520:n WAN-portilta sisään tulevaa liikennettä, josta myös muiden palvelimien liikenteen piti kulkea. Listassa oli valmiiksi esimerkin 2 mukaiset säännöt:

```
access-list 104 remark auto generated by SDM firewall configuration##NO_ACES_14##
access-list 104 remark SDM_ACL Category=1
access-list 104 deny   ip 10.1.10.0 0.0.0.3 any
access-list 104 deny   ip 192.168.10.0 0.0.0.255 any
access-list 104 deny ip 10.1.1.0 0.0.0.255 any
access-list 104 permit udp host 10.95.254.252 eq domain any
access-list 104 permit icmp any host 10.95.1.240 echo-reply
access-list 104 permit icmp any host 10.95.1.240 time-exceeded
access-list 104 permit icmp any host 10.95.1.240 unreachable
access-list 104 deny   ip 10.0.0.0 0.255.255.255 any
access-list 104 deny   ip 172.16.0.0 0.15.255.255 any
access-list 104 deny   ip 192.168.0.0 0.0.255.255 any
access-list 104 deny   ip 127.0.0.0 0.255.255.255 any
access-list 104 deny   ip host 255.255.255.255 any
access-list 104 deny   ip host 0.0.0.0 any
access-list 104 deny   ip any any log
```

Esimerkki 2. Pääsylistan 104 alkuperäiset säännöt.

Trixboxilta tulevien pakettien hylkäys näkyi ilmoituksena UC520:n komentoliittymässä mutta Call Managerilta tulevien pakettien osalta ilmoitusta ei näkynyt. Selitys siihen lienee se, että Call Managerin paketit pysähtyivät esimerkin 2 ylempään punaisella merkittyyn sääntöön, kun taas Trixboxin paketit pysähtyivät vasta viimeiseen sääntöön. Pääsylistan sääntö ”deny ip 192.168.0.0 0.0.255.255 any” kieltää kaikki ip-paketit 192.168.-alkavista osoitteista kohdeosoitteesta riippumatta, mikä täsmää Call Managerista tulevaan pakettiin. Viimeinen sääntö ”deny ip any any log” kieltää kaikki ip-paketit lähde- ja kohdeosoitteesta riippumatta sekä näyttää tapahtumasta syslog-viestin. Koska mikään aiempi sääntö ei täsmännyt Trixboxin osoitteen kanssa, pysähtyivät paketit viimeiseen sääntöön. Ongelma ratkaistiin tekemällä pääsylistaan 2 uutta sääntöä listan 104 alkupäähän:

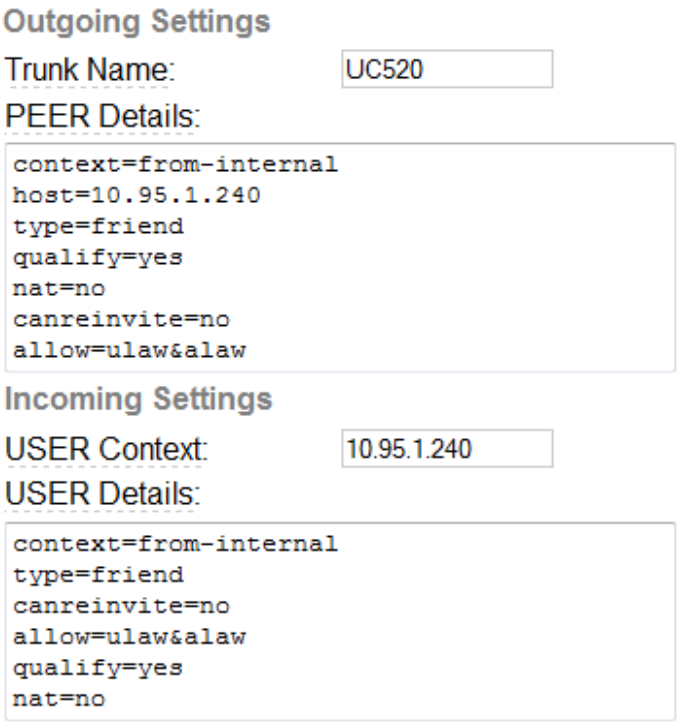
- access-list 104 permit ip host 193.167.199.83 any
- access-list 104 permit ip host 192.168.9.2 any

Ensimmäinen sääntö sallii kaikki ip-paketit Trixboxilta ja alempi Call Managerilta. Tietoturvan kannalta säännöistä saisi tehtyä paremmat sallimalla vain tarkoitukseen pakolliset protokollat. Tietoturvallisessa laboratorioympä-

ristössä päädyttiin kuitenkin vain selvittämään pakettien kulkuun liittyvä ongelma ja lähinnä tiedostamaan tietoturvaan liittyvät seikat.

6.3.2 Trixboxin asetukset

Trixboxiin konfiguroitiin aiempien yhteyksien tapaan SIP-trunk-linkki (Kuva 38) ja lähtevä reitti. trunk-linkkiin sisältyvien käskyjen selitykset löytyvät sivuilta 40 ja 47. Lähtevän reitin asetuksiin tuli numerokaavaksi UC520:ssa käytettyjen puhelinnumeroiden yleinen muoto 2XXX.



Kuva 38. Trixbox-UC520-trunk-linkin konfiguraatio

6.4 Call Manager ja UC520

Tavoite palvelinten välisen tiedonkulun sovittamisessa oli sama kuin muissakin edellä mainituissa tapauksissa Puheluiden soittaminen molempiin suuntiin piti saada onnistumaan yksivaiheisesti.

6.4.1 Call Manager

Asetusten teko koostui jälleen trunk-linkin ja reitin määrittelystä. Toimenpiteet olivat kohde-IP-osoitetta, SIP-liikenteen UDP-porttinumeroa ja Route

pattern -määrityksen numerokoodia lukuun ottamatta samanlaiset kuin luvussa 6.2.1.

SIP-liikenteen UDP-porttinumeroksi vaihdettiin 5062, sillä Trixbox ei hyväksynyt tälle samaa porttinumeroa (5060) kuin aikaisemmassa Trixbox-Call Manager -määrittelyssä. Tämä johtuu Call Managerin ominaisuuksista vaatia jokaiselle SIP-trunk linkille oma porttinumeronsa [t].

6.4.2 UC520

Esimerkistä 3 näkyy, että SIP-yhteysasetusten konfiguroiminen Call Manageria varten tehtiin samoilla komennoilla kuin Trixboxin tapauksessa. Ainoastaan yhteyksille yksilölliset parametrit muutettiin. Komentojen selitykset näkyvät esimerkistä 1 sivulla 52.

dial-peer voice 200 VoIP

*description **TO CCM***

destination-pattern 3...

session protocol sipv2

session target ipv4:192.168.9.2

dtmf-relay rtp-nte

codec g711alaw

no vad

Esimerkki 3. UC520:n SIP-yhteysasetukset Call Managerille

6.5 Puhelimet ja muut asetukset

VoIP-palvelinten ja SIP-merkinannon toimintaa testattiin rekisteröimällä jokaiseen palvelimeen ainakin 1 puhelin. Pitkät viiveet ja virheet puheluiden muodostuksessa indikoivat yleensä virheellisistä tai puutteellisista laiteasetuksista kun kyseessä on järjestelmän rakennusvaihe. Fyysisiä laitevikoja ei työn aikana ilmennyt.

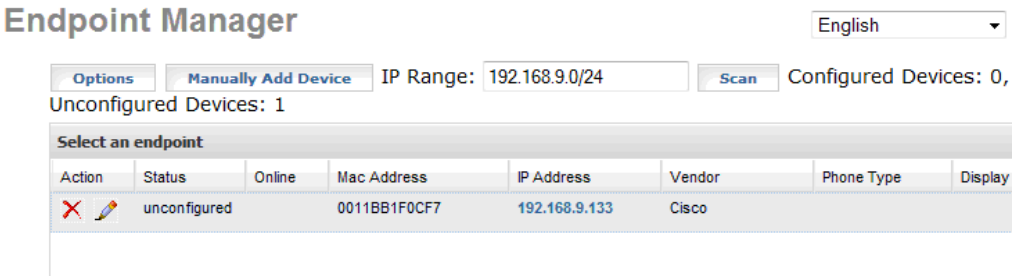
6.5.1 Puhelimet

Puhelinten asennus suoritettiin rekisteröimällä kukin niistä johonkin käytetyistä palvelimista. Ciscon palvelimiin asetettiin puhelimen mac-osoite ja malli. Trixboxiin laitettiin käyttäjänimi ja salasana. Trixboxiin liitettyihin puhelimiin piti lisäksi asettaa Trixboxin IP-osoite tai verkkotunnus. UC520:n asetuksissa jokaiselle puhelimelle oli määritettävä myös käyttäjänimi. Näin vastaanottavan puhelimen näkyi numeron lisäksi myös oletetun käyttäjän tai omistajan nimi. IP-osoitteensa puhelimet saivat automaattisesti DHCP-palvelinten avulla, jotka toimivat laboratorioluokan reitittimissä ja kytkimissä sekä UC520:ssa.

6.5.2 Endpoint Manager

Tässä työssä Trixboxiin asennetulla Endpoint Manager -moduulilla puhelinten etsiminen lähiverkosta käy helposti, eikä niiden ip-osoitteita tai mahdollisia verkkotunnuksia tarvitse muistaa ulkoa. Löydettyjen puhelinten web-pohjaiselle konfigurointisivulle pääsee helposti linkin kautta. Moduuli asennettiin testimielessä, mutta sen huomattiin helpottavan myös työtä.

Kuva 39 havainnollistaa etsinnän toimivuutta. Haku 192.168.9.0/24 verkosta on löytänyt Ciscon ip-puhelimen, joka on rekisteröity vain Call Managerin kanssa. Sinisellä tekstillä olevaa IP-osoitetta klikkaamalla päästään puhelimen web-sivulle.



Kuva 39. Puhelinten etsintä Endpoint managerin avulla

7 YHTEENVETO JA LOPPUTULOKSET

Lukuisten testien ja asetusten säätämisen jälkeen järjestelmän laitteet saatiin keskustelemaan keskenään ja puhelut kulkivat kaikin puolin sujuvasti. Laboratorioluokassa sijainneet 3 VoIP-palvelinta hoitivat signaloinnin vauhdikkaasti ja lopulta järjestelmä oli niin nopea, että puhelimet alkoivat hälyttää käytännössä samalla hetkellä, kun viimeisen numeron painallus tapahtui. Suurin viive syntyi mobiiliverkon osalta, mutta sekään ei ollut normaalia suurempi, joten yhdyskäytävän suorittama liikenteen muunto oli ilmeisen ripeää.

Työn keskeisin asia oli SIP-signalointiin ja laitteiden konfigurointiin perehtyminen. Parhaiten tietoa löytyi internetin kautta erilaisten aihetta koskevien foorumeiden kautta, sillä käyttöohjeista ei paljoa apua ollut muutamia virallisia dokumentteja lukuun ottamatta. Trixboxin osalta virallista käyttöohjetta ei ole, Call Manageria koskevista Ciscon dokumentaatioista ei löydetty apua signaloinnin sovittamiseen ja Portechin dokumentaatio auttoi lähinnä mobiiliverkon ja VoIP-verkon asetusten säätämisessä. UC520:n graafinen käyttöliittymä oli looginen ja laitteen käyttöönotto onnistui ilman ohjetta. Sip-asetusten säätäminen vaati kuitenkin laitekohtaisten termien ja asetusten selvittelyä.

Työn keskittyessä lähinnä VoIP-palvelinten yhteensovittamiseen, jäi kehittämisen varaa erityisesti palveluiden ja tietoturvan osalta. Yhtenä kokeilematta jääneenä asiana olivat videopuhelut. Vaikka pöytäpuhelimet eivät niitä tukeneetkaan, olisi niiden käyttö ohjelmistopuhelimilla ollut mahdollista. Älykkäät VoIP-palvelinohjelmistot tarjoavat myös monia muita hyödyllisiä lisäpalveluita, jotka jäivät tämän työn ulkopuolelle. Niistä löytyisi varmasti vielä ainakin yhden lopputyön ainekset.

VIITELUETTELO

[1] Cisco. Waveform Coding Techniques [verkkodokumentti]. 2006 [viitattu 13.5.2011]. Saatavissa: http://cisco.com/application/pdf/paws/8123/waveform_coding.pdf.

[2] Teleware Oy. IP-puhe. Koulutusmateriaali. Helsinki: Metropolia ammattikorkeakoulu. 1999.

[3] Cisco. Understanding Codecs: Complexity, Hardware Support, MOS, and Negotiation. [verkkodokumentti]. 2006 [viitattu 30.5.2011]. Saatavissa: http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a00800b6710.shtml.

[4] Internet Engineering Task Force. RFC 3261 SIP [verkkodokumentti]. 2002 [viitattu 15.5.2011]. Saatavissa: http://tools.ietf.org/html/rfc3261.

[5] Cisco. Guide to Cisco Systems' VOIP Infrastructure Solution for SIP [verkkodokumentti]. 2000 [viitattu 19.5.2011]. Saatavissa: http://www.cisco.com/application/pdf/en/us/guest/tech/tk587/c2001/ccmigration_09186a00800eadf1.pdf.

[6] Viestintävirasto [verkkodokumentti]. 16.3.2010 [viitattu 20.5.2011]. Etusivu > Puhelin > Puhelinverkon numerointi > Matkaviestinverkkojen suuntanumerot. Saatavissa: http://www.viestintavirasto.fi/index/puhelin/puhelinverkonnumerointi/matkaviestinverkkojensuuntanumerot.html

[7] Cisco. Internet Protocols [verkkodokumentti]. 2009 [viitattu 4.6.2011]. Saatavissa: http://docwiki.cisco.com/wiki/Internet_Protocols.

[8] Aki Tikkala, Jatkuva-aikaisten multimediasovellusten kehitysalusta. Diplomityö. VTT. Elektroniikka. Espoo. 2002.

[9] Internet Engineering Task Force. RFC 4566 SDP [verkkodokumentti]. 2006 [viitattu 31.5.2011]. Saatavissa: http://tools.ietf.org/rfc/rfc4566.

[10] W3C. SMIL 3.0 [verkkodokumentti]. 2008 [viitattu 15.5.2011]. Satavissa: http://www.w3.org/TR/SMIL3/.

[11] Mark Collier. Basic vulnerability issues for SIP security [verkkodokumentti]. 2005 [viitattu]. Saatavissa: http://www.securityvibes.com/servlet/JiveServlet/previewBody/1275-102-1-1275/SIP_Security030105.pdf.

[12] Cisco. Voice Over IP – Per Call Bandwidth Consumption [verkkodokumentti]. 2006 viitattu [4.6.2011]. Saatavissa: http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml.

[13] Cisco. Understanding delay in Packet Voice Networks [verkkodokumentti]. 2006 [viitattu 6.6.2011]. Saatavissa: http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00800a8993.shtml.

[14] Cisco. Getting Started Guide Cisco Unified Communications 500 Series Model UC 520 [verkkodokumentti]. Saatavissa: http://www.cisco.com/en/US/docs/voice_ip_comm/sbcs/uc500/hardware/quick/guide/UC520_QSG.pdf

[15] Uplinx [verkkodokumentti]. 2008 [11.7.2011]. Uplinx Online Shop > Cisco Products > Cisco Routers – VoIP Gateways > UC520-8U-2BRI-K9. Saatavissa: http://www.uplinx.com.au/catalog/cisco-cme-base-cue-and-phone-w2bri-1vic-p-40.html

[16] Cisco. Session Initiation Protocol Gateway Call Flows and Compliance Information [verkkodokumentti]. 2002 [viitattu 11.7.2011]. Saatavissa: http://www.cisco.com/application/pdf/en/us/guest/products/ps4032/c2001/ccmigration_09186a00800c4bb1.pdf

SIP-VASTAUSVIESTIT [16]

1xx = tietoa sisältävät vastaukset
• 100 Pyyntöä käsitellään
• 180 Puhelinyhteyttä luodaan
• 181 Soittoa välitetään eteenpäin
• 182 Pyyntö odottaa käsittelyä
• 183 Soiton tila
2xx = pyyntöjen onnistumiset
• 200 OK
• 202 hyväksytty: Käytetään viitteitä varten
3xx = uudelleenohjaukset
• 300 Useita vaihtoehtoja
• 301 Siirretty pysyvästi
• 302 Siirretty väliaikaisesti
• 305 Käytä välityspalvelinta
• 380 Vaihtoehtoinen palvelu
4xx = pyyntöjen epäonnistumiset
• 400 Virheellinen pyyntö
• 401 Ei valtuuksia: Ainoastaan rekisteröijien käytössä. Välityspalvelimien on käytettävä välityspalvelimen valtuutusta 407.
• 402 Maksua vaaditaan (tulevaa käyttöä varten)
• 403 Kielletty
• 404 Ei tulosta: Käyttäjää ei löytynyt
• 405 Metodi ei sallittu
• 406 Kelpaamaton
• 407 Välityspalvelimen tunnistusta vaaditaan
• 408 Pyynnön aikakatkaisu: Käyttäjää ei löytynyt ajoissa
• 410 Poistunut: Käyttäjä oli olemassa, mutta ei ole enää saatavilla.
• 413 Pyynnön pituus liian suuri
• 414 Pyyntö-URI liian pitkä
• 415 Mediatyyppi ei tuettu
• 416 URI-kaava ei tuettu
• 420 Laajennusvirhe: Virheellinen SIP-protokollan laajennus, palvelin ei ymmärtänyt sitä.
• 421 Laajennusta vaaditaan
• 423 Aikaväli liian lyhyt
• 480 Väliaikaisesti ei saatavilla
• 481 Puhelua/transaktiota ei olemassa
• 482 Silmukka havaittu
• 483 Liian monta hyppyä
• 484 Osoite epätäydellinen
• 485 Epäselvä
• 486 Varattu
• 487 Pyyntö lopetettu
• 488 Ei sallittu tässä

• 491 Pyynnön käsittely käynnissä
• 493 Ei luettavissa: S/MIME -osa ei luettavissa
5xx = palvelinvirheet
• 500 Palvelimen sisäinen virhe
• 501 Ei suoritettu: SIP-pyynnön metodia ei suoriteta tässä
• 502 Yhdyskäytävävirhe
• 503 Palvelua ei saatavilla
• 504 Palvelimen aikakatkaisu
• 505 Versiota ei tueta: Palvelin ei tue tätä SIP-protokollan versiota
• 513 Viesti liian suuri
6xx = maailmanlaajuiset häiriöt
• 600 Kaikkialla varattu
• 603 Torjuttu
• 604 Ei olemassa
• 606 Kelpaamaton