VOIP:IN KÄYTETTÄVYYS

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto
Opinnäytetyö
Syksy 2007
Lotta Kurkela

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

KURKELA,LOTTA: VoIP:in käytettävyys

Tietoliikennetekniikan suuntautumisvaihtoehdon opinnäytetyö, 37 sivua

Syksy 2007

TIIVISTELMÄ

Työ käsittelee VoIP-järjestelmän testausta ja VoIPin perusteita. VoIP–järjestelmän testauksen tarkoituksena on auttaa kehittämään Elisan asiakaspalveluratkaisuja. Järjestelmä perustuu Click-To-Call periaatteeseen: asiakas voi soittaa asiakaspalvelijalle VoIP–järjestelmää käyttäen selvittääkseen ongelmia itsepalvelukeskuksessa. Tämä tapahtuu valitsemalla linkki internet-sivustolla.

VoIP muodostuu sanoista Voice over IP. Tämä tarkoittaa puhelun muodostamista internetin yli normaalin lanka- tai mobiiliverkon sijaan. On olemassa useita erilaisia standardeja VoIP-puheluiden muodostamiseen, joista yleisimmin käytettyjä ovat SIP ja H.323.

Tämä työ keskittyy erilaisten laitteisto- ja selainkokoonpanojen yhteensopivuuden testaukseen.

Testaukset tehtiin asentamalla eri Windows versioita erilaisiin pöytä- ja kannettaviin tietokoneisiin. Tämän jälkeen suosituimmat selaimet asennettiin käyttöjärjestelmiin, ja testaukset suoritettiin näillä.

Tämän perusteella tehtiin lista yhteensopivista järjestelmistä. Testien perusteella selvisi, että palvelu ei toimi alle 16kbps nopeuksilla. Tämän lisäksi näitä tuloksia voidaan käyttää tämän järjestelmän kehittämisen tukena.

Avainsanat: VoIP, Testaus, Selain, Flash

Lahti University of Applied Sciences
Faculty of Technology

KURKELA, LOTTA: Usability of VoIP

Bachelor's Thesis in Information Technology, 37 pages

Autumn 2007

ABSTRACT

This thesis deals with the basics of VoIP and VoIP system testing. The purpose of the VoIP system being tested is to help the development of Elisa's customer service solutions. The system is based on the so-called Click-To-Call principle: a customer could call to a customer service representative by using the VoIP system to get help for problems concerning self service. This can be done by selecting the link in a web page.

VoIP stands for Voice over IP. This means making phone calls by using internet or local area networks instead of normal landlines or a mobile phone. There are a few different standards for initiating VoIP calls. The most widely used ones are SIP and H.323.

In the study the testing was concentrated on the compatibility of different hardware, browser and operating system combinations that customers might have with this particular service. Tests were done by installing different versions of Microsoft Windows operating systems on different kinds of desktop and laptop computers. Then the most popular browsers were installed on these operating systems and the system was tested with these.

Based on this, a list of compatible systems was made. The tests showed that the connection did not work under 16kbps speed. Also, these results can be used to support the further development of the system.

Keywords: VoIP, Testing, Browser, Flash

SISÄLLYS

LYHENTEET

3G	Third Generation, kolmas matkapuhelin sukupolvi.
ADSL	Asymmetric Digital Subscriber Line, tiedonsiirtotekniikka.
AES	Advanced Encryption Standard, lohkosalausmenetelmä.
ARP	Address Resolution Protocol, Ethernet-verkossa käytettävä protokolla, joka selvittää IP-osoitetta vastaavan MAC-osoitteen.
CAT-5	Category-5, kaapelointistandardi.
DES	Data Encryption Standard, lohkosalausmenetelmä.
DDoS	Distributed-Denial-of-Service, hajautettu palvelunestohyökkäys.
DoS	Denial-of-Service, palvelunestohyökkäys.
GPRS	General Packet Radio Service, GSM-verkossa toimiva pakettikytkentäinen tiedonsiirtopalvelu.
GSM	Groupe Spécial Mobile, matkapuhelintekniikka.
HMAC-SHA1	Hash Message Authentication Code-Secure Hashing Algorithm 1, kryptografinen salausmenetelmä, jolla varmistetaan sanoman muuttumattomuus.
HTTP	Hypertext Transfer Protocol, hypertekstin siirtoprotokolla.

IEEE	Institute of Electrical and Electronics Engineers, kansainvälinen tekniikan alan järjestö.
IETF	Internet Engineering Task Force, Internet-protokollien standardoinnista vastaava organisaatio.
IP	Internet Protocol, tiedonsiirtoprotokolla.
ISDN	Integrated Services Digital Network, piirikytkentäinen puhelinverkkojärjestelmä.
ISUP	ISDN User Part, ISDN-merkinanto.
ITU	International Telecommunication Union, tietoliikenneasioita hallinnoiva kansainvälinen organisaatio.
ITU-T	ITU Telecommunication Standardization Sector, ITU:n työryhmä, joka vastaa uusien standardien määrittelystä.
MAC	Media Access Control, verkkosovittimen Ethernet-verkossa yksilöivä osoite.
MCU	Multipoint Control Unit, verkossa oleva laite, joka mahdollistaa kolmen tai useamman päätelaitteen välisen liikennöinnin.
MDCP	Media Device Control Protocol, protokolla jolla ohjataan erilaisia medialaitteita.
MGCP	Media Gateway Control Protocol, VoIP-yhdyskäytävien ohjaamisessa käytettävä protokolla.
MMUSIC	Multiparty Multimedia Session Control, IETF:n työryhmä, joka kehittää telekonferenssi-protokollia.

NAT	Network Address Translation, staattinen osoitteenmuunnos.
PSTN	Public Switched Telephone Network, yleinen puhelinverkko.
QoS	Quality of Service, palvelun laatu.
RAS	Registration, Admission and Status, rekisteröinti, pääsynhallinta ja tilatieto.
RC4	Rivest Cipher 4, salausalgoritmi.
RFC	Request for Comments, Internet-standardien kokoelma.
RSA	Rivest Shamir Adleman, salausalgoritmi, joka on nimetty kehittäjien mukaan.
RTCP	Real-Time Transport Control Protocol, tietoliikenneprotokolla.
RTMP	Real-Time Messaging Protocol, Adoben kehittämä protokolla äänen, videon ja datan reaaliaikaiseen siirtämiseen internetin yli.
RTP	Real-Time Transport Protocol, reaaliaikainen tiedonsiirtoprotokolla.
RTSP	Real Time Streaming Protocol, tiedonsiirtoprotokolla.
RTT	Round-Trip Time, paketin kulkuaika verkossa.
SCIP	Simple Conference Invitation Protocol, SIP:in edeltäjä.
SIP	Session Initiation Protocol, IP-puhelinyhteyksien luonnista vatsaava tietoliikenneprotokolla.
S/MIME	Secure/Multipurpose Internet Mail Extensions, salausmenetelmä.

SMTP	Simple Mail Transfer Protocol, TCP pohjainen sähköpostin siirtoon tarkoitettu protokolla.
SRTP	Secure Real-Time Transport Protocol, suojattu reaaliaikainen tiedonsiirtoprotokolla.
SSL	Secure Sockets Layer, salausprotokolla.
TCP	Transmission Control Protocol, tietoliikenneprotokolla.
TLS	Transport Layer Security, SSL, salausprotokolla.
UDP	User Datagram Protocol, tietoliikenneprotokolla.
UMTS	Universal Mobile Telecommunications System, kolmannen sukupolven matkapuhelin teknologia.
VLAN	Virtual Local Area Networks, virtuaalinen lähiverkko.
VoIP	Voice over IP, IP-puhe.
VPN	Virtual Private Network, suojattu verkkoyhteys.
WAN	Wide Area Network, laajaverkko.

1 JOHDANTO

Elisa Oyj on valtakunnallinen teleoperaattoriyritys. Elisan toiminta on alkanut vuonna 1882 Helsingin puhelimena. Vuosien myötä yritykseen sulautui useampia paikallisia puhelinoperaattoreita sekä maailman ensimmäinen GSM (Groupe Spécial Mobile) -operaattori Radiolinja. Vuonna 2000 Helsingin puhelin muutti nimensä Elisaksi. Elisan päämarkkina-alue on Suomi, mutta kansainvälistä toimintaa on myös Virossa. Elisa on listautunut pörssiyhtiöksi vuonna 1997. Konsernin henkilöstömäärä vuonna 2006 oli n. 3600 henkeä. Vuoden 2006 lopussa konsernin verkossa oli 1,3 miljoonaa kiinteän verkon liittymää joista n. 500000 oli laajakaistaliittymiä. Matkapuhelinliittymiä oli n. 2,5 miljoonaa kappaletta. Liikevaihto vuonna 2006 oli 1,52 miljardia euroa.

Centile on 1998 perustettu ranskalainen yritys, joka tarjoaa erilaisia VoIP (Voice over Internet Protocol) -järjestelmiä palveluntarjoajille. Yhtiön päätuote on IntraSwitch niminen VoIP-järjestelmä, jota yhtiö on kehittänyt yli kuusi vuotta.

Tämän opinnäytetyön tavoitteena on testata Centilen Click-To-Call järjestelmän yhteensopivuutta erilaisten käyttöjärjestelmä- ja selain yhdistelmien kanssa sekä näiden käytettävyyttä. Työn tutkimustavoitteena on selvittää miten järjestelmää voidaan tulla käyttämään osana Elisan asiakaspalveluratkaisuja ja näin ollen parantamaan asiakkaan saamaa palvelua.

Työssä tehtävät testit rajattiin tällä hetkellä yleisimmin käytössä oleviin selaimiin ja käyttöjärjestelmiin. Testit tehtiin sekä kannettavilla- että pöytätietokoneilla.

VoIP:sta on tehty useita opinnäytetöitä, mutta kirjallisuustutkimusta tehtäessä ei löytynyt vastaavanlaista opinnäytetyötä, jossa olisi testattu yksittäisen alustan käytettävyyttä erilaisilla laitteistokokoonpanoilla.

2 VOIP

2.1 Yleistä

VoIP (Voice over Internet Protocol) on yleinen nimitys puheensiirtoon tietoverkkojen kautta reaaliajassa. Puhe muutetaan digitaaliseksi päätelaitteessa ja siirretään verkon yli pakettimuotoisena datana. Puhelut, jotka reitittyvät perinteiseen lanka- tai matkapuhelinverkkoon, kulkevat yhdyskäytävän kautta.

VoIP-puhelu koostuu merkinantoprotokollasta sekä puheensiirtoon käytetystä protokollasta. Merkinantoprotokolla (esim. SIP (Session Initiation Protocol)) huolehtii puhelun muodostamiseen, ylläpitoon sekä päättämiseen tarvittavasta signaloinnista. Puheensiirtoon käytettävä protokolla (esim. RTP (Real-Time Transport Protocol)) huolehtii puheen siirrosta eri puhelun osapuolien välillä.

VoIP:in sovellutuksia normaaleiden puheluiden lisäksi ovat esimerkiksi Call Center-järjestelmät sekä PSTN (Public Switched Telephone Network)-keskusten välinen runkoverkkoliikenne.

2.1.1 Käytännössä huomioitavat asiat

Yrityskäytössä korvattaessa normaali puhelinverkko IP (Internet Protocol)-puhelimilla, tulee huomioida seuraavat asiat: Lähiverkon on oltava vähintään CAT-5 (Category-5)-standardin mukaisesti kaapeloitu 100Mbps Ethernet-kytkinverkko. Verkossa käytettyjen kytkinten tulee tukea 802.1Q (VLAN, Virtual Local Area Network) ja 802.1p (QoS, Quality of Service) –protokollia, jotta puhelinlaitteet saadaan laitettua omaan VLANiinsa ja jotta VoIP-liikenteelle voidaan taata tietty palvelulaatu. Lisäksi verkon aktiivilaitteita (kytkimet ja reitittimet) tulee valvoa, jotta mahdollisiin ongelmiin voidaan puuttua nopeasti. Mikäli halutaan liikennöidä myös yrityksen lähiverkon ulkopuolelle VoIP:illa, tulee myös ulkoverkkoon suuntautuvasta yhteydestä (WAN, Wide Area Network) varata riittävästi kaistaa. Liikennöitäessä yleiseen puhelinverkkoon liikenteen tulee kulkea erillisen gateway-laitteiston kautta. Käytettävissä olevan kaistan

puute tai tiedonsiirron laatuvaatimusten toteutumattomuus aiheuttaa puheluiden laadun heikkenemistä. Liikennöinnin tapahtuessa yrityksen toimipisteiden välillä on huomioitava liikenteen priorisointi ns. kultaluokka ja liikenteelle on varattava oma laskennallinen kaista.

2.2 SIP

2.2.1 Yleistä

SIP (Session Initiation Protocol) on IETF (Internet Engineering Task Force):n kehittämä signalointiprotokolla, joka huolehtii multimedia-istuntojen muodostamisesta, avoimen yhteyden muokkaamisesta ja yhteyden purkamisesta. Sillä voidaan myös olemassa olevaan istuntoon kutsua uusia käyttäjiä tai lisätä istuntoon uusia käytettäviä medioita. Koska SIP toimii ainoastaan signalointiprotokollana, se ei ota kantaa istunnon sisältöön, joka voi olla puhetta, videota, tekstisanomia tai jaettu työpöytä. Istuntojen kuvaamiseen käytetään pääsääntöisesti SDP (Session Description Protocol) –protokollaa, mutta myös mitä tahansa muuta kuvausprotokollaa voidaan käyttää. SIP on HTTP (Hypertext Transfer Protocol)-protokollaan perustuva tekstipohjainen protokolla, joka on suunniteltu avoimeksi ja joustavaksi. (RFC 3261 2002.)

2.2.2 Historia

SIPin historia alkaa helmikuussa 1996. Tällöin Mark Handley ja Eve Schooler julkaisivat MMUSIC (Multiparty Multimedia Session Control) -työryhmän tuottaman luonnosteludokumentin yksinkertaisesta protokollasta, jolla voidaan kutsua käyttäjiä osallistumaan internetin välityksellä tapahtuviin multimedia konferensseihin. Tälle protokollalle annettiin nimi Session Invitation Protocol (SIP), myöhemmin tästä alettiin käyttää nimitystä SIPv1. Tässä versiossa nähtiin riittäväksi, että protokolla toimi ainoastaan istuntojen muodostamiseen käyttäen tiedonsiirtoon UDP (User Datagram Protocol)-protokollaa sekä SDP-protokollaa apuna istuntokuvauksissa. (Session Invitation Protocol 1996.)

Samana päivänä myös Henning Schulzrinne julkaisi oman luonnoksen protokollasta, jonka käyttötarkoitus oli sama. Tämä protokolla oli nimeltään SCIP (Simple Conference Invitation Protocol) ja oli suunniteltu HTTP- ja SMTP (Simple Mail Transfer Protocol)-protokollien lähtökohdista. Sen ajatuksena oli hyväksi käyttää jo olemassa olevaa sähköposti-infrastruktuuria käyttämällä sähköpostiosoitteita käyttäjien tunnuksina. SCIP käyttää tiedonsiirtoon TCP (Transmission Control Protocol)-protokollaa. (Simple Conference Invitation Protocol 1996.)

Joulukuussa 1996 Handley, Schulzrinne ja Schooler julkaisevat yhdessä luonnoksen dokumentista, jossa kuvataan Session Invitation ja Simple Conference Invitation –protokollien ominaisuuksia yhdistävästä protokollasta, jolle annettiin nimi Session Initiation Protocol, josta käytetään myös nimitystä SIPv2. Tämän dokumentin pyrkimys on kehittää protokollasta yksinkertaisempi ja laajennettavampi. Tämä versio protokollasta käyttää sekä TCP ja UDP-protokollia tiedonsiirtoon. UDP:n käyttö on suositeltua tiedonsiirron tehokkuuden kannalta, kun taas TCP on joustavampi palomuurien suhteen. (Session Initiation Protocol 1996.)

Ensimmäinen virallinen määritys SIP:stä julkaistiin vuonna helmikuussa 1999. Tämän dokumentin tekemiseen osallistui alkuperäisten tekijöiden lisäksi myös J. Rosenberg. Tämä dokumentti on IETF:n julkaisema standardi RFC(Request for Comments) 2543. Protokolla jatkoi kehittymistä ja siitä julkaistiin kesäkuussa 2002 uudempi standardi, RFC 3261, joka korvasi alkuperäisen määrittelyn. Protokollan saatua suuren mielenkiinnon, IETF perusti SIP-työryhmän syyskuussa 1999, sen tehtävä on hallinnoida protokollan ja tämän laajennosten kehittymistä. (Session Initiation Protocol 1996.)

2.2.3 Arkkitehtuuri

SIP-arkkitehtuuri jakautuu kahteen osaan: käyttäjän agenttiin (user agent) ja palvelimeen (server). Käyttäjän agentti toimii puhelun päätepisteenä (osapuolena) istunnossa, sekä aloittavana että vastaanottavana osapuolena. Agentti jakautuu

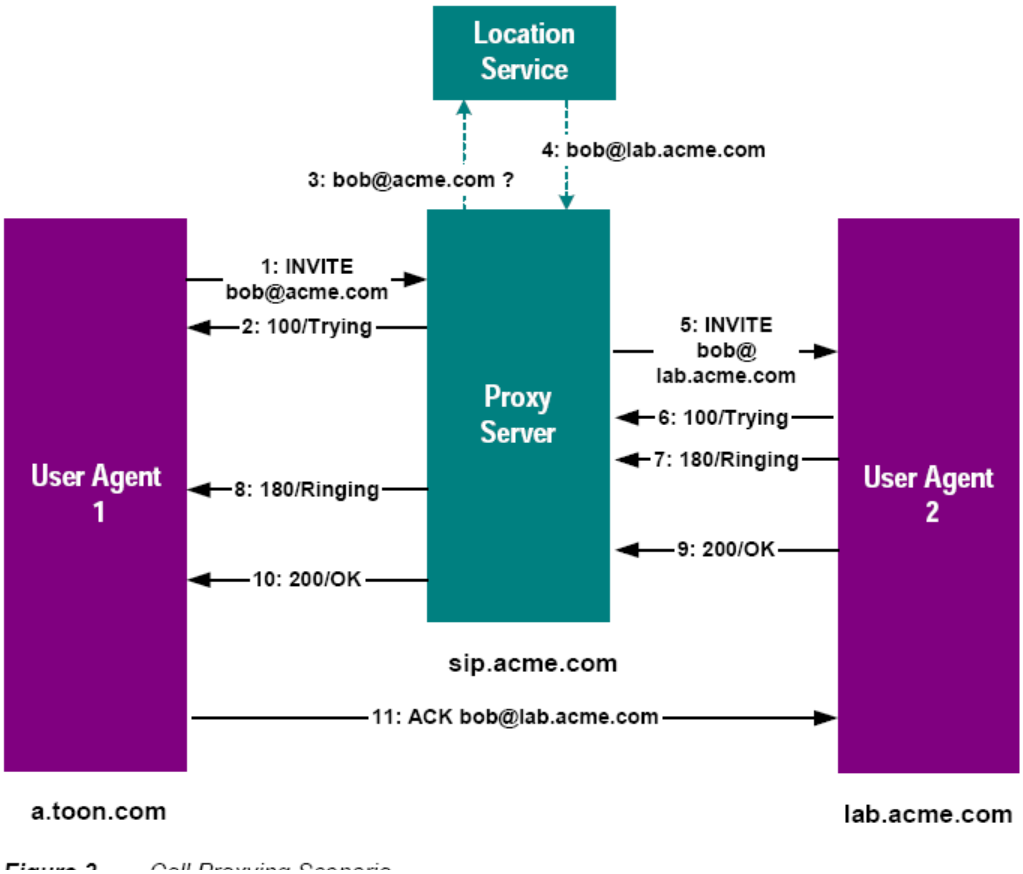
puolestaan kahteen osaan: palvelin- ja asiakas-osaan. Agentin asiakasosa huolehtii lähtevien pyyntöjen luomisesta. Pyyntöjen saapuessa käyttäjälle, agentin palvelinosa huolehtii näihin vastaamisesta. Sekä asiakas- että palvelinosa tekevät päätökset käyttäjän valintojen tai muiden syötteiden perusteella. Agentin asiakasosa lähettää välityspalvelimelle pyynnön, joka välitetään edelleen joko suoraan vastaanottavan agentin palvelinosalle tai useamman muun välityspalvelimen kautta. Vastaanottavan agentin palvelinosa vastaa saamaansa pyyntöön, ja tämä vastaus välitetään takaisin pyynnön lähettäneen agentin asiakasosaan. Käyttäjän agentti on usein tietokoneeseen asennettu puhelinsovellus, mutta tämä voi olla myös lähiverkkoon kytketty puhelinkone, kämmenmikro tai julkiseen puhelinverkkoon kytketty yhdyskäytävä. (Porter 2006, 154-156.)

Palvelimen tehtävä on käyttäjätunnusten yhdistäminen IP-osoitteisiin, jotta sanomat agenttien välillä voidaan toimittaa. Käyttäjän agentti rekisteröityy SIP palvelimelle, jotta käyttäjä voidaan paikantaa ja muut käyttäjät näkevät, onko käyttäjä kirjautuneena järjestelmään sekä mahdollistaa sanomien toimittamisen käyttäjän senhetkiseen sijaintiin. Koska käyttäjät eivät aina tiedä toisten osapuolien senhetkistä sijaintia, hoidetaan muiden käyttäjien kutsuminen istuntoon lähettämällä pyyntö käyttäjän agentilta palvelimelle. Palvelin selvittää, onko toinen osapuoli liittyneenä samaan palvelimeen kuin jolle pyyntö on tullut ja tarvittaessa välittää pyynnön edelleen seuraavalle palvelimelle, jolla käyttäjä pitäisi sijaita. SIP-palvelimella on kolme roolia: rekisteröinti-, välitys- ja ohjauspalvelin. (Porter 2006, 155-157.)

Rekisteröintipalvelin pitää kirjaa palvelimelle rekisteröityneistä käyttäjistä ja näiden IP-osoitteista ja tallentaa ne paikkapalvelimelle. Kun käyttäjä halutaan kutsua istuntoon, pyydetään rekisteröintipalvelimelta tieto käyttäjän sen hetkisestä sijainnista sekä tieto, onko käyttäjä rekisteröityneenä palveluun. Paikkapalvelin on yleensä osa fyysistä rekisteröintipalvelinta, mutta tämä voi sijaita myös muualla verkossa. (Porter 2006, 156.)

Välityspalvelin vastaanottaa sanomia muilta verkon käyttäjiltä ja välittää ne edelleen toisille käyttäjän agenteille tai toisille SIP-palvelimille. Välityspalvelin

voi toimia myös pääsynhallinta-, tunnistus- ja valtuutuspalvelimena. (Porter 2006, 156.)

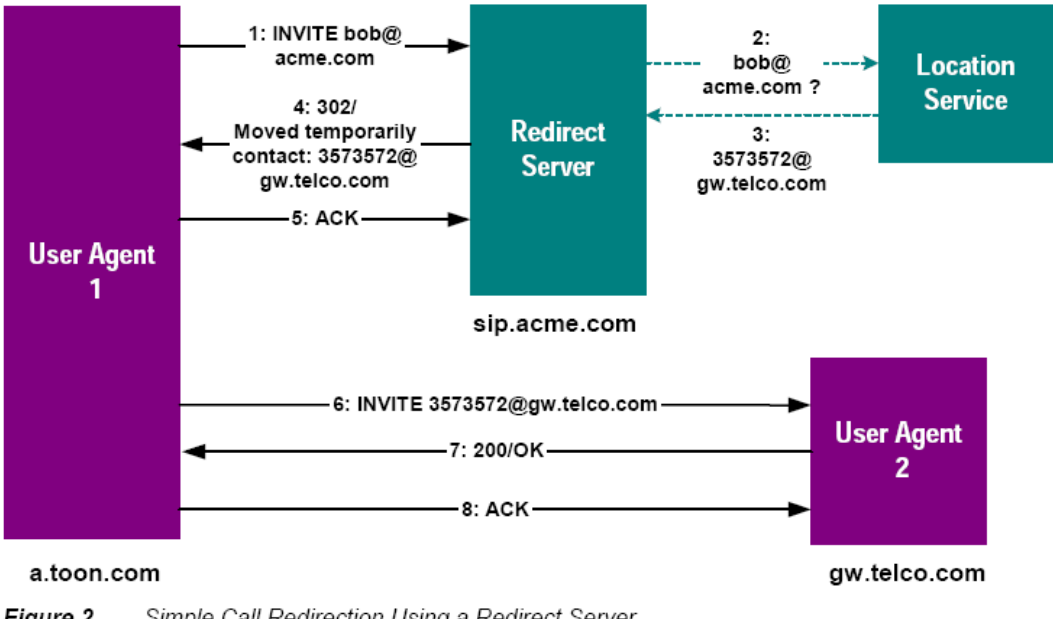


KUVIO 1. Esimerkki SIP yhteyden muodostamisesta välityspalvelimen kautta (Radvision 2005, 12.)

Käyttäjä 1 osoitteesta a.toon.com haluaa muodostaa istunnon käyttäjän 2 kanssa. Käyttäjän 1 agentti lähettää INVITE-pyynnön yhteyden muodostamiseksi. Agentti saa käyttäjän 2 SIP-palvelimen osoitteen selville nimipalvelukyselyn avulla. Tässä esimerkissä palvelimen osoite on sip.acme.com. Tälle palvelimelle lähetetään käyttäjän 2 agentille suunnattu INVITE-pyyntö. Palvelin vastaanottaa INVITE-pyynnön ja kuittaa kutsuvalle agentille, että yhteyttä yritetään muodostaa. Tämän

jälkeen välityspalvelin ottaa yhteyden paikkapalvelimen käyttäjän 2 agentin rekisteröidyn osoitteen selvittämisestä varten. Paikkapalvelin palauttaa käyttäjän 2 agentille rekisteröidyn osoitteen ja välityspalvelin lähettää INVITE-pyynnön tähän osoitteeseen. Vastaanottava agentti saa pyynnön ja vastaa puhelun muodostuksen olevan käynnissä. Nyt käyttäjän 2 agentti hälyttää käyttäjälle tulevasta kutsusta sekä ilmoittaa välityspalvelimelle, joka puolestaan ilmoittaa kutsuvalle agentille, että kutsutun käyttäjän agentti hälyttää. Kun käyttäjä vastaa tulevaan kutsuun, lähettää agentti tilavasteen 200 hyväksytyn kutsun merkiksi. Välityspalvelin lähettää myös tämän onnistumista kuvaavan vasteen alkuperäiselle kutsujalle. Kutsuva agentti lähettää ACK-sanoman suoraan kutsutulle agentille muodostuneen puhelun merkiksi (Radvision 2005, 13).

Ohjauspalvelin vastaanottaa sanomia muilta verkon käyttäjiltä, mutta toisin kuin välityspalvelin, ohjauspalvelin ei välitä sanomaa edelleen vaan palauttaa sanoman lähettäneelle palvelimelle tai käyttäjän agentille tiedon vastaanottavan käyttäjän agentin sijainnista, jolloin sanoman lähettäjä kommunikoi suoraan vastaanottajan kanssa ilman välikäsiä. Ohjauspalvelin voi tarvittaessa myös jakaa käyttäjälle saapuvan kutsun useampaan eri osoitteeseen. Tällöin mikäli käyttäjä on rekisteröitynyt palvelimelle usealla eri agentilla, jakaa ohjauspalvelin saapuvan kutsun kaikille agenteille, jotka ilmoittavat saman aikaan saapuvasta kutsusta. Kun saapuvaan kutsuun vastataan jostain agentista, menee tieto vastauksesta muille agenteille ja nämä lopettavat. (Porter 2006, 156-157.)



KUVIO 2. Esimerkki SIP yhteydenmuodostamisesta ohjauspalvelimen kautta (Radvision 2005, 11.)

Ohjaustapauksessa SIP-palvelin palauttaa jälleenohjausta kuvaavan 300 –luokan vasteen yhteydenmuodostuskutsuun. Vastauksessa on kutsutun agentin yhteysosoite Contact header –kentässä. Kutsuva agentti hyväksyy vastauksen ACK-vasteella palvelimelle yhteyden päättymisen merkiksi. Kutsuva agentti lähettää seuraavaksi uuden INVITE-pyynnön palvelimen antamaan osoitteeseen. Jos kutsu onnistuu, jatketaan istunnon muodostamista normaaliin tapaan. (RFC 3261 2002; Porter 2006, 156-162.)

SIPin käytössä tietoverkoissa on kaksi pääongelmaa: palomuurit sekä NAT (Network Address Translation)-osoitemuunnos. Palomuurien säännöstöön on helppo määritellä SIP-protokolla sallituksi, sillä se käyttää vakioasetuksissa liikennöintiin porttia 5060. Ongelmaksi muodostuu istunnon liikenteen siirtoon käytettävä RTP-protokolla. RTP-protokolla koostuu erillisistä data- ja ohjausliikenteestä. RTP ei käytä liikennöintiin ennalta määriteltäviä portteja, vaan portit määritellään dynaamisesti vasta liikennöinnin alkaessa agenttien välillä. Näin ollen palomuureihin ei voida ennalta määritellä sääntöjä tämän liikenteen sallimiseksi. (Lintula 2004, 12.)

NAT-muunnoksessa sisäverkosta julkiseen verkkoon suuntautuvaa liikennettä muokataan palomuurissa niin, että kaikki sisäverkosta ulos suuntautuva liikenne näyttää tulevan samasta osoitteesta. SIP liikenteen kannalta tämä on ongelmallista, sillä tällöin SIP-sanomien sisällä olevat IP- ja portti-tiedot eivät enää vastaakaan julkisessa verkossa kulkevaa sanomaa, eikä verkon ulkopuolelta pystytä ottamaan yhteyttä sisäverkossa olemaan koneeseen tämän sisäverkon osoitteella. (Lintula 2004, 12.)

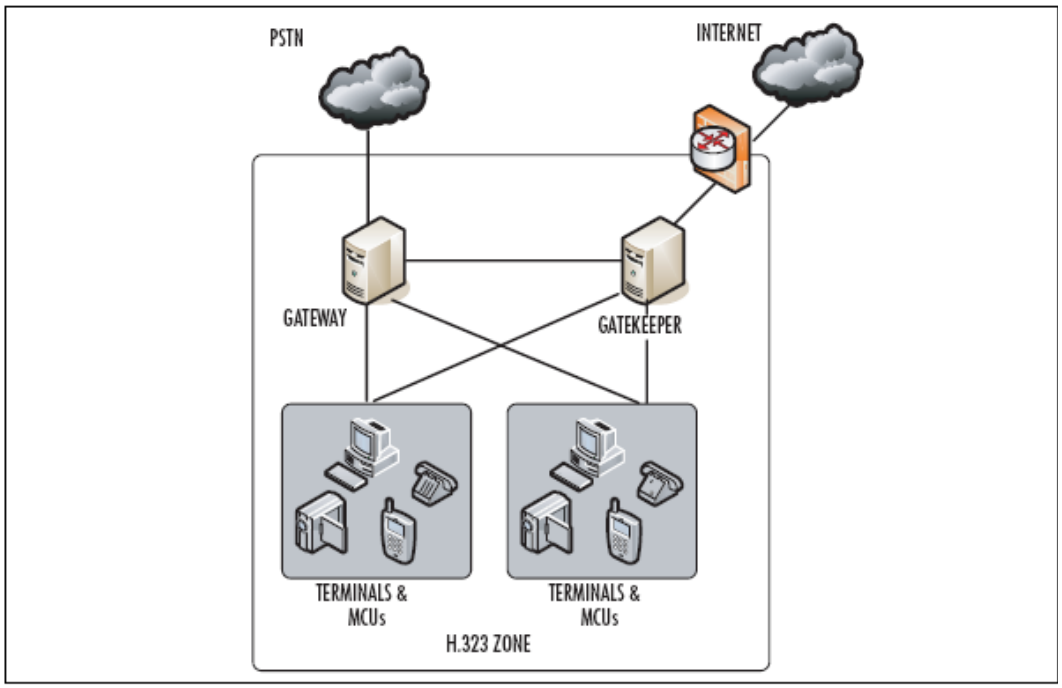
SIP perustuu HTTP-protokollaan, jossa asiakas- ja palvelinohjelmistojen välillä lähetetään pyyntöjä, joihin vastataan ennalta määrätyillä vastearvoilla. Tärkeimmät pyynnöt ovat REGISTER, INVITE, ACK, OPTIONS, SUBSCRIBE, NOTIFY, CANCEL ja BYE. Kun agentti käynnistetään, se lähettää ensimmäisenä REGISTER-kutsun palvelimelle, jolla tämä rekisteröityy rekisteröintipalvelimelle ja käyttäjän tiedot lisätään sijaintipalvelimelle. INVITE-sanomalla agentti kutsuu toisen agentin mukaan istuntoonsa. ACK-sanomalla hyväksytään istunto ja vahvistetaan sanomaliikenne. OPTIONS-sanoma agentti voi pyytää lisätietoja toisen agentin tukemista toiminnallisuuksista. Tätä käytetään, jotta voidaan varmistua siitä, että vastaanottava agentti kykenee liittymään haluttuun istuntoon. Tämän jälkeen kuitenkin kutsuva agentti joutuu vielä erikseen lähettämään INVITE-sanoman, mikäli vastapää halutaan kutsua istuntoon. NOTIFY-sanomalla agentti päivittää omaa tilaansa palvelimelle. CANCEL-sanomalla agentti vastaa kielteisesti saapuneeseen pyyntöön, mutta jo auki olevaa istuntoa ei suljeta. BYE-sanomalla agentti purkaa avoimen istunnon. Sanoman voi lähettää sekä istunnon luonut että siihen liittynyt agentti missä tahansa istunnon vaiheessa. (RFC 3261 2002; Porter 2006, 159-162.)

Kun palvelin tai toinen agentti on vastaanottanut pyynnön agentilta tai palvelimelta, vastataan siihen kolminumeroisella vastekoodella, kuten HTTP-protokollassakin. Vastekoodit on jaoteltu kuuteen luokkaan koodin ensimmäisen numeron perusteella. 1xx –sarjan koodit ovat ilmoitusluonteisia (informational), niillä kuitataan saapunut sanoma vastaanotetuksi ja käsittelyssä olevaksi. 2xx –sarja ilmaisee hyväksyttyä vastausta sanomalle (success). 3xx –sarja ilmaisee uudellenohjaustilannetta (redirect), jossa kutsuvan agentin on reagoitava vasteen mukana tulleeseen lisätietoon ja on sen mukaisesti lähetettävä uusi kutsu. 4xx –

sarjan vasteet kertovat virheestä saapuneessa pyynnössä (client error). 5xx –sarjan vasteet kertovat sanoman vastaanottaneella palvelimella tapahtuneesta virheestä (server error). 6xx –sarjan virheilmoitukset ilmaisevat virheen joka estää pyynnön käsittelyn verkon kaikilla palvelimilla (global error). (RFC 3261 2002; Porter 2006, 160-162.)

2.3 H.323

H.323 protokolla mahdollistaa erilaisten laitteiden kommunikoinnin keskenään. H.323 tukee reaaliaikaista ääni-, video- ja dataliikennettä. Tuki ääniliikenteelle on pakollinen, kun taas data ja video ovat valinnaisia. H.323 määrittelee neljä erilaista toiminnallista yksikköä, jotka muodostavat H.323 verkon. Nämä komponentit sisältävät päätepisteet (päätelaite, endpoint), yhdyskäytävät (gateway), portinvartijat (gatekeeper) ja monipistehallintayksiköt (Multipoint control unit, MCU). (Porter 2006, 124-126.)



KUVIO 3. Esimerkki H.323 verkosta (Porter 2006, 125.)

Päätepisteet ovat tyypillisesti laitteita joita loppukäyttäjät käyttävät (puhelimet, puhelinohjelmat, IVR:t, vastaajapalvelut, videokamerat jne.). Päätepisteet tarjoavat ainoastaan ääni- ja/tai multimediapalveluita, kuten videoneuvottelu ja ohjelmistojen yhteiskäyttö. (Porter 2006, 124-126.)

Yhdyskäytävät hoitavat signaloinnin ja tiedonsiirron, ja yhdyskäytävä on valinnainen toiminnallisuus H.323 verkossa. Mikäli verkossa on portinvartija, yhdyskäytävä on yhteydessä tähän ja portinvartija huolehtii yhteyksien reitittämisestä eri yhdyskäytävien kautta. Yhdyskäytävä toimii rajapintana eri verkkojen välillä, kuten ISDN (Integrated Services Digital Network), PSTN tai toiset H.323 verkot. Yhdyskäytävä hoitaa muunnoksen esimerkiksi H.323:sta SIP:iin tai ISUP (ISDN User Part):iin eli mahdollistaa pakettikytkentäisen verkon liittämisen piirikytkentäiseen verkkoon. (Porter 2006, 124-126.)

Portinvartijat hoitavat osoitemuunnoksen ja pääsynhallinnan H.323 verkossa. Sen tärkein tehtävä on hoitaa osoitteenmuunnos symbolisten- ja IP-osoitteiden välillä. Tällöin on mahdollista soittaa käyttäjälle ”Matti”, ilman että tarvitsee tietää tämän päätelaitteen IP-osoitetta. Portinvartija hallinnoi päätepisteiden pääsyä palveluihin, verkkoresursseihin ja voivat myös tarjota muita lisäpalveluita. Ne valvovat palveluiden käyttöä ja tarjoavat verkon kaistan käytön hallintaa. Portinvartija ei ole pakollinen osa H.323 verkkoa, mutta mikäli sellainen on, päätelaitteiden on käytettävä portinvartijan palveluita. Portinvartijan ja yhdyskäytävän toiminnallisuudet ovat usein samassa laitteessa. (Porter 2006, 124-126.)

Monipistehallintayksiköt (MCU, Multipoint Control Unit) tarjoaa kolmen tai useamman päätepisteen välistä konferenssipalvelua. H.323 määrittely mahdollistaa erilaisia konferenssipalveluita joko keskitettyinä tai hajautettuina. (Porter 2006, 124-126.)

Taustapalvelimet ovat tärkeä lisäosa H.323 ympäristöä. Nämä tarjoavat mm. autentikointi-, valtuutus-, laskutus- ja hinnoittelupalveluita. Yksinkertaisimmissa

verkoissa yhdyskäytävä tai portinvartija hoitaa nämä tehtävät (Porter 2006, 124-126.)

H.323 –protokollapino sisältää useita erillisiä protokollia, jotka mahdollistavat palveluiden tarjoamisen käyttäjille. Yhteydenmuodostamisen kannata tärkeimpiä protokollia ovat H.225, H.235, H.245 ja Q.900-sarjan signalointiprotokollat. Perustiedonsiirrossa tukeudutaan RTP ja RTCP (Real-Time Transport Control Protocol)-protokolliin. H.225/Q.931 määrittelee yhteyden muodostuksessa ja purussa käytettävän signaloinnin ja signaloinnin yhteydessä välitettävät yhteysparametrit. H.225.0/RAS määrittelee signalointiin, rekisteröintiin, pääsynhallintaan ja tilatietoon (Registration, Admission and Status) sekä tietovirran kuvaukseen käytettävät sanomat. H.245 puolestaan määrittelee sanomat, joilla osapuolet neuvottelevat päätteiden ominaisuudet, asiakas-palvelin –suhteen ja tietovirran siirtoon käytettävän loogisen kanavan ominaisuudet. (Porter 2006, 126-129.)

Puheensiirtoon H.323 tarjoaa useampia koodekeita puheen siirtämiseen. Yksi vanhimpia koodekeita on G.711, jota käytetään myös julkisessa puhelinverkossa ja ISDN-puhelimissa puheen siirtoon. Tämä koodekki tarvitsee reilusti siirtokaistaa eikä tue pakkausta. G.723.1 on video- ja puhelinkonferensseihin suunniteltu koodekki, joka optimoitu nopeaksi signaalin purun ja pakkaamisen suhteen. VoIP käyttöön on suunniteltu G.729 koodekki, jossa on optimoitu siirtoon tarvittavan kaistanleveys mahdollisimman pieneksi. (Porter 2006, 127.)

Signalointiliikenne reititetään yleensä portinvartijan kautta tai portinvartijan päätöksellä suoraan osapuolien välillä. Tietovirta reitittyy yleensä suoraan osapuolien välillä tai yhdyskäytäviä käyttäen. Tiedonsiirtoon käytetään sekä TCP- ja UDP-protokollia. Tiedonsiirron luotettavuuden kannalta parempi TCP-protokolla huolehtii signaloinnin ja ohjausdatan siirrosta varmistaen, että kaikki lähetetyt paketit saapuvat perille varmasti ja oikeassa järjestyksessä. UDP-protokollaa käytetään siirtämään audio- ja videovirtoja osapuolien välillä, kun sanomien riittävän nopea kulkuaika osapuolien välillä on tärkeämpää kuin se, että kaikki paketit saapuvat perille. Näin ollen on siis luontevaa, että H.225 ja H.245 –protokollat sekä RTCP-protokolla käyttävät liikennöintiin TCP-protokollaa ja

H.225/RAS ja RTP-protokollat liikennöivät UDP-protokollalla. (Porter 2006, 127-129.)

Yhteyden muodostaminen H.225-protokollalla jakautuu kahteen osaan, kutsun signalointiin ja RAS-osuuteen. Signalointi määrittelee tavat yhteyden muodostamiseen, ylläpitoon ja purkamiseen. Q.931 –signalointisanomia käytetään muodostamaan H.323 päätepisteiden välisiä yhteyksiä, joita pitkin istunnoissa käytetty reaaliaikainen data, kuten video tai puhe, tullaan siirtämään. Ennen muiden yhteyksien muodostamista, avataan signalointikanava päätepisteen ja yhdyskäytävän, kahden yhdyskäytävän tai yhdyskäytävän ja portinvartijan välille. Mikäli verkossa ei ole yhdyskäytävää tai portinvartijaa, H.225 sanomat välitetään suoraan päätepisteiden välillä. H.225 määrittelee myös päätepisteen ja portinvartijan sekä kahden portinvartijan väliset sanomat, joita kutsutaan H.225:n RAS-osaksi. RASia käytetään rekisteröitymiseen, pääsynhallintaan ja kaistanleveyden hallintaan verkossa sekä yhteyden purkuun päätelaitteen ja portinvartijan välillä. RAS-sanomien välittämiseen käytetään omaa kanavaa, joka on erillään puhelunmuodostamiseen käytetystä kanavasta. Tämä toinen kanava avataan päätelaitteen ja portinvartijan välille ennen uusien yhteyksien muodostamista. (Porter 2006, 129-134.)

Kahden päätepisteen välille istuntoa muodostettaessa suoraan, avataan näiden välille kaksi TCP-yhteyttä, toinen istunnon muodostamista varten H.225/Q.931 sanomia käyttäen ja toinen istunnon hallintaan ja toiminnallisuuksien tiedonvaihtoa varten H.245 sanomin. Toinen päätepiste aloittaa H.225/Q.931 sanomien vaihdon toisen päätepisteen kanssa. Sanomien vaihdon jälkeen vastaanottavan päätepiste hälyttää saapuvasta istunnosta. Onnistuneen puhelun muodostamisen jälkeen päätepisteet vaihtavat H.245 sanomia, joiden avulla päätepisteet neuvottelevat tiedonsiirrossa käytettävät parametrit. (Porter 2006, 126-141.)

H.245 sanomia käytetään selvittämään istunnossa käytetyn median tyyppi, päätelaitteiden tukemat ominaisuudet sekä muodostamaan yhteys tiedonsiirtoon ennen varsinaisen istunnon muodostamista. H.245 hallinnoi istunnon parametreja istunnon muodostamisen jälkeen. H.245 ohjauskanava säilyy pysyvästi avoimena

koko istunnon ajan, toisin kuin istunnossa käytetyt mediakanavat. H.245 käyttää omaa siirtoyhteyttä sanomien vaihtoon, mutta osa toteutuksista käyttää H.225:n siirtoyhteyttä H.245 sanomien välittämiseen, jolloin päätelaitteiden välille muodostetaan vain yksi siirtoyhteys istunnon hallintaa varten. (Porter 2006, 126-141.)

Onnistuneen neuvottelun päätteeksi istunto on muodostettu ja päätelaitteiden välille muodostettu istunto on valmis käytettäväksi. Mikäli verkossa käytetään portinvartijaa, edeltää H.225/Q.931 signalointia H.225 RAS signalointi, jolla päätelaite rekisteröityy verkkoon ja pyytää lupaa istunnon muodostamiseen. (Porter 2006, 126-141.)

2.4 RTP

RTP (Real-Time Transport Protocol) eli tosiaikainen kuljetusprotokolla on pakettikytkentäisissä tietoverkoissa käytetty protokolla, jolla kuljetetaan tosiaikasta tiedonsiirtoa vaativaa dataa, kuten ääntä ja videota. RTP on yksinkertainen protokolla, joka tarjoaa sovellukselle tiedon protokollan kuljettaman tiedon tyypistä, ajoituksesta sekä siirron valvonnasta. RTP käyttää tiedonsiirrossa UDP-kuljetuskerrosta, joka mahdollistaa paremman tiedonsiirtokapasiteetin, sillä pakettien perille pääsyä ei tarvitse valvoa, koska RTP:tä käyttävät sovellukset kykenevät toimimaan vaikka osa paketeista katoaisikin siirrossa. Protokolla on suunniteltu niin, että sitä käyttävät sovellukset huolehtivat itse siirrettävän tiedon pilkkomisista soveltuvan kokoisiin paketteihin siirtoa varten sekä mahdollisesti kadonneiden pakettien uudelleenlähettämisen, mikäli sovellus ei kykene muutoin toipumaan kadonneista paketeista. Protokolla ei myöskään huolehdi siitä, että lähetetyt paketit saapuvat vastaanottajalle oikeassa järjestyksessä vaan jättää sitä käyttävän sovelluksen vastuulle huolehtia pakettien järjestämisestä oikeaan järjestykseen käyttöä varten protokollan tarjoaman ajoitustiedon perusteella. Ajoitustietoa voidaan käyttää myös paketin lopullisen sijainnin määrittämiseen ilman, että paketit tarvitsee käsitellä järjestyksessä. Tätä voidaan hyödyntää esimerkiksi silloin, kun samaa siirtoyhteyttä käytetään vaikkapa sekä puheen että videon siirtoon. RTP-

protokollaan käytetään tietoverkkojen VoIP-liikenteen lisäksi myös 3G (Third Generation)-matkapuhelinverkoissa puheluihin sekä multimedian siirtoon. (RFC3550 2003.)

RTP-protokollan yhteydessä käytetään RTCP-protokollaa (Real-Time Transport Control Protocol) tukemaan tiedon siirtoa. RTCP luo oman yhteyden RTP-protokollaa käyttävien osapuolien välille. RTCP lähettää säännöllisin väliajoin ohjaustietoa osapuolien välillä, tärkeimpänä on kertoa tiedonsiirron laadusta. RTCP kerää tietoa osapuolien välillä siirretyn tiedon määrästä tavuina ja paketteina, kadonneiden pakettien määrästä, kulkuaikojen vaihtelusta (jitter) sekä kokonaiskulkuajasta (RTT, Round Trip Time). Sovellus voi hyödyntää tätä tietoa yrittääkseen parantaa siirron laatua vaikkapa muuttamalla lähetettyjen pakettien kokoa tai lähetysnopeutta. (RFC3550 2003.)

2.5 SDP

SDP (Session Description Protocol) eli istunnon kuvausprotokollaa käytetään verkossa siirrettävien multimediaistuntojen, kuten ip-puheluiden tai videokuvan, kuvaamiseen. SDP suunniteltiin alun perin reaaliaikaisten multimediaesitysten kuvaamiseen MBONEa (Multicast Backbone) käytettäessä. SDP esittää siirron ajankohdan, siihen kuuluvan sisällön (ääni, video, grafiikka) ja niihin kuuluvat parameterit (siirtoprotokolla, ääni/video koodekki, IP-osoitteet ja porttinumerot). SDP sisältää ainoastaan tiedon istunnon sisällöstä, eikä se ota kantaa tiedonsiirtoon. SDP ei sisällä siirtoprotokollaa, vaan se on tarkoitettu siirrettäväksi jonkin toisen protokolla, kuten HTTP, SIP tai RTSP (Real Time Streaming Protocol,), sisällä. (RFC 4566 2006) (RFC 3264 200x).

SIPiä varten SDP:hen on toteutettu neuvotteluprotokolla (Offer/Answer Model with SDP), jolla voidaan luoda uusia tai muokata olemassa olevia puheluita. Tämä laajennus on suunniteltu erityisesti käytettäväksi silloin, kun tiedonsiirrossa käytetään multicast-tekniikkaa. (RFC 4566 2006) (RFC 3264 200x).

2.6 Muut

2.6.1 Skype

Muita on esim. Skype, joka on täysin suljettu verkko, jonka protokolla on salainen. Skype on ilmainen sovellus, jolla voi internetin yli soittaa äänipuheluita, videopuheluita ja lähettää pikaviestejä. Skype perustuu Peer To Peer –tekniikkaan, jossa puhelut reitittyvät muiden verkon käyttäjien kautta Ensimmäinen versio Skypestä julkaistiin heinäkuussa 2004 ja elokuussa 2005 sillä arvioitiin olevan 54 miljoonaa käyttäjää. Syyskuussa 2005 Yhdysvaltalainen eBay nettihuutokauppa osti Skypen n. 3 miljoonan yhdysvaltain dollarilla. (Porter 2006, 184-186.)

Puhelun muodostus Skypessä voi alkaa, kun molemmat osapuolet ovat kirjautuneet Skypen kirjautumispalvelimelle. Kirjautumisyhteys on salattu käyttäen 256-bittistä AES (Advanced Encryption Standard) -protokollaa. Kirjautumisen jälkeen pääte avaa yhteyden johonkin verkossa olevaan supernodeen. Supernodena voi toimia mikä tahansa verkkoon liittynyt pääte, jolla on käytettävissään riittävästi ylimääräistä tehoa, muistia ja verkkoliikenne kapasiteettia. Puhelua muodostettaessa pääte kysyy supernodelta toisen osapuolen sijainnin. Mikäli molemmilla osapuolilla on käytössää julkinen IP-osoite, voidaan yhteys muodostaa suoraan osapuolien välillä. Mikäli soittaja sijaitsee NAT-osoitemuunnoksen tekevän palomuurin takana, reititetään signaloinnin TCP-yhteys supernoden kautta ja osapuolien välinen UDP-liikenne suoraan. Mikäli molemmat osapuolet ovat palomuurien takana eivätkä kykene muodostamaan välilleen suoraan yhteyttä, reititetään kaikki liikenne supernoden kautta. (Baset 2004.)

Vaikka Skype on käyttäjän kannalta helppokäyttöinen, eikä kärsi monien muiden VoIP-protokollien tapaan palomuurien aiheuttamista ongelmista, ei sen käyttöön monen yrityksen tai oppilaitoksen tietohallinnossa suhtauduta positiivisesti. Tämä johtuu siitä, että mikäli päätelaitteella on käytettävissä tarvittavat resurssit, saattaa se nousta verkon supernodeksi. Supernode välittää liikennettä verkkoon kytkeytyneiden päätteiden välillä, jotka eivät pysty liikennöimään suoraan toisen

päätelaitteiden välillä niiden edessä olevien palomuurien takia. Tämä aiheuttaa ylimääräistä verkkoliikennettä, joka kuormittaa verkkoa, jossa supernode sijaitsee. Vaikka Skypeä ei käytettäisikään aktiivisesti, riittää sovelluksen päällä olo siihen, että se reitittää muiden liikennettä taustalla käyttäjän tietämättä ja syö käytettävissä olevaa kapasiteettia muilta käyttäjiltä ja mahdollisesti aiheuttaa lisäkustannuksia. Toinen asia, joka aiheuttaa negatiivista suhtautumista Skypeen on tämän erittäin tarkoin varjeltu lähdekoodi ja protokolla. Koska tarkkaa tietoa Skypen toiminnasta ei ole annettu julkisuuteen, ei kukaan pysty sanomaan varmaksi, kuinka luotettavaa sen toiminta on. Vaikka liikenne verkossa onkin vahvasti salattua, ei voida silti voida olla varmoja, etteikö tiedot voisi päätyä jonkun kolmannen osapuolen tietoon. Myös sovelluksen turvallisuudesta on esitetty useita eri mielipiteitä, sillä jotkut tahot ovat epäilleet että sovellus kertoisi koneella olevista tiedoista eteenpäin. (Baset 2004.)

2.6.2 H.248

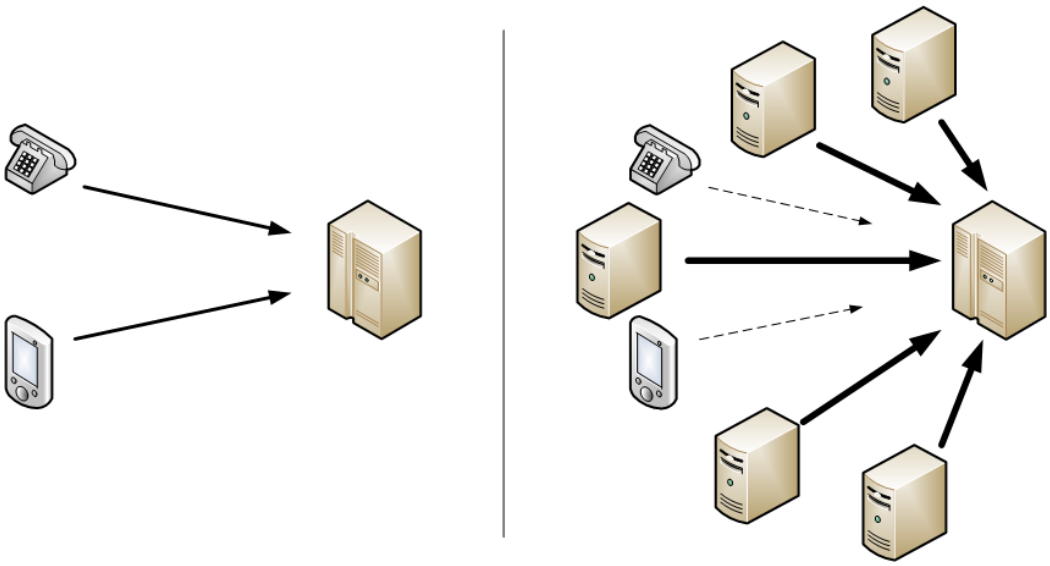
H.248 (tunnetaan myös nimeltä Megaco) –protokollaa käytetään mediayhdyskäytävän ja mediayhdyskäytäväohjaimen väliseen liikennöintiin VoIP-verkoissa. Yhdellä mediayhdyskäytäväohjaimella voi ohjata yhtä tai useampaa mediayhdyskäytävää tämän protokollan avulla. Mediayhdyskäytävällä hoidetaan VoIP-liikennettä kahden eri IP-verkon välillä sekä IP- ja PSTN-verkon välillä. H.248 standardi on IETF- ja ITU (International Telecommunication Union)-organisaatioiden yhteinen tuotos, joka perustuu IETF:n MGCP (Media Gateway Control Protocol)- ja ITU-T:n MDCP (Media Device Control Protocol) -protokolliin. Protokollan tavoite oli ratkaista ongelmat VoIP- ja PSTN-verkkojen yhdistämisessä. (RFC3525 2003; Porter 2006, 189-190.)

3 VOIPIN TIETOTURVA

3.1 Uhat

VoIP-järjestelmiä suunniteltaessa ja ylläpidettäessä on kiinnitettävä erityistä huomiota tietoturvallisuuteen. Tietoverkossa liikkuva puhelinliikenne on huomattavasti perinteistä puhelinverkkoa suuremmassa vaarassa joutua erilaisten riskien kohteeksi, varsinkin jos VoIP-liikenne kulkee samassa verkossa kuin muu tietoliikenne.

Palvelunestohyökkäys (Denial-of-Service, DoS) voidaan kohdistaa mihin tahansa tietoliikenteeseen tai sen yksittäiseen palveluun tai palvelimeen. Palvelunestohyökkäyksellä voidaan joko heikentää tarjotun palvelun laatua tai estää tämän käyttö kokonaan. Palvelunestohyökkäyksessä kohteen palvelutasoa pyritään heikentämään lähettämään tälle enemmän yhdenaikaisia pyyntöjä, kuin mitä tämä pystyy käsittelemään. Tällöin kohde ei kykene enää tarjoamaan palveluitaan oikeille käyttäjilleen. Täydelliseen palvelunestoon tarvitaan usein useampia hyökkääjiä, jotta hyökkäävällä taholla on käytettävissään enemmän resursseja kuin kohteena olevalla taholla. Tällaista hyökkäystä kutsutaan hajautetuksi palvelunestohyökkäykseksi (Distributed-Denial-of-Service, DDoS). Hyökkäyksen kohteena voi olla joko yksittäinen palvelu, kuten websivusto. Tällöin web-palvelinta kuormitetaan lähettämällä mahdollisimman paljon erilaisia pyyntöjä, jotta palvelinsovellus joutuu tekemään mahdollisimman paljon työtä yksittäistä pyyntöä kohti. Tietoliikenneyhteyksiä voidaan häiritä luomalla siirtoyhteydelle ylimääräistä liikennettä enemmän, kuin mikä on käytettävissä oleva siirtokapasiteetti. Tällöin reitittimiltä kuluu resursseja häirintäliikenteen käsittelyyn ja vastauspakettien lähettämiseen, jolloin asialliselle liikenteelle jäävä kapasiteetti putoaa hyvin pieneksi tai estyy täydellisesti. (Porter 2006, 240-247; VOIPSA Threat Taxonomy Wiki 2006.)



KUVIO 4. Palvelunestohyökkäys.

Mikäli VoIP-liikenne kulkee samassa verkossa kuin muu tietoliikenne, estää tällainen tietoliikenteeseen kohdistuva palvelunestohyökkäys myös verkossa kulkevan VoIP-liikenteen. Vastaavasti tällöin voidaan hyökätä myös verkossa olevaa VoIP-palvelinta vastaan, jolloin voidaan heikentää palvelun käytettävyyttä. VoIP-liikenne on erittäin altis palvelunestohyökkäykselle, sillä VoIPin puheensiirto tarvitsee reaaliaikaista tiedonsiirtoa, jotta puheensiirtoon käytetyt paketit pääsevät perille sekä riittävän varmasti ja nopeasti. (Porter 2006, 240-247; VOIPSA Threat Taxonomy Wiki 2006.)

Kuviossa 4 esitetään palvelunestohyökkäyksen periaate. Kuvion vasemmassa reunassa on esitetty normaali tilanne, jolloin päätelaitteet kommunikoivat verkossa olevan yhdyskäytävän kanssa normaalisti. Kuvion oikeassa reunassa esitetään hajautettu palvelunestohyökkäys, jossa samaan verkkoon kytketyt laitteet pommittavat yhdyskäytävää luomalla tälle suuntautuvaa ylimääräistä liikennettä. Ylimääräinen liikenne kuormittaa yhdyskäytävän tietoliikennekapasiteettia, jolloin oikeiden käyttäjien liikenne ei pääse haittaliikenteen takia yhdyskäytävälle riittävällä varmuudella, jolloin yhdyskäytävän kautta kulkevat puhelut eivät onnistu. (Porter 2006, 240-247; VOIPSA Threat Taxonomy Wiki 2006.)

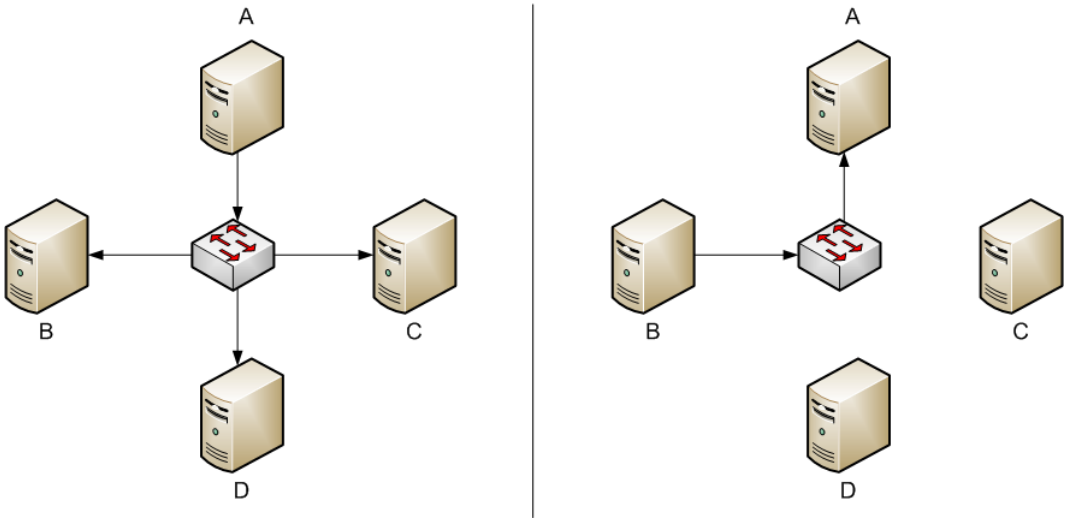
Palvelunestohyökkäystä vastaan on hankala suojautua, sillä hyökkäys perustuu hyökkääjän generoimaan valtavaan liikennemäärään, joka käsittely vie kohteelta käytettävissä olevat resurssit. Palvelunestohyökkäyksen vaikutuksia voidaan pyrkiä minimoimaan verkkosuunnittelulla. Suurin hyöty saavutetaan erottamalla VoIP-liikenne omaan verkkonsa, erilleen muusta verkkoliikenteestä. Tällöin muussa liikenteessä tapahtuvat hyökkäykset eivät pääse häiritsemään VoIP-verkon liikennettä. Myös jakamalla verkko useampaan segmenttiin, voidaan minimoida hyökkäyksen vaikutuksia. Tällöin yhden segmentin ylikuormittuminen ei estä muissa segmenteissä liikennöintiä. (Porter 2006, 240-247; VOIPSA Threat Taxonomy Wiki 2006.)

Toinen merkittävä uhka VoIP:lle on puheluiden salakuuntelu ja kaappaus. Salakuuntelussa kolmas osapuoli pystyy seuraamaan ja tallentamaan kaikki osapuolien välillä liikkuvat sanomat mutta ei voi tai halua muuttaa liikenteen sisältöä. Kaappauksessa kolmas osapuoli vaikuttaa osapuolien väliseen liikenteeseen. (RFC826 1982.)

Kytkentäisessä Ethernet-verkossa paketit reititetään verkkosovittimen MAC-osoitteen (Media Access Control) perusteella vain lähde- ja kohdekoneiden välillä, ainoastaan levityssanomat lähetetään kaikille lähiverkkoon kytketyille laitteille. Kun laite haluaa keskustella samassa verkossa sijaitsevan toisen laitteen kanssa, lähettää tämä paketit tämän laitteen MAC-osoitteella varustettuna verkkoon, jolloin verkon aktiivilaitteet toimittavat paketit oikealle laitteelle. Jotta laite voi lähettää paketin, on tämän ensin selvitettävä vastaanottajan MAC-osoite. Tämä tapahtuu ARP-protokollan (Address Resolution Protocol) avulla, tämä esitetään kuviossa 5. (RFC826 1982.)

Osoitteen selvittäminen tapahtuu lähettämällä verkkoon ARP-levityssanoma, jossa lähettävä kone tiedustelee samassa lähiverkossa sijaitsevan IP-osoitetta käyttävän laitteen MAC-osoitetta. Kuvion 5 vasemmalla puolella olevassa tilanteessa kone A lähettää koko verkolle suunnatun levityssanoman, jolla tiedustelee IP-osoitteen 192.168.255.20 omistajaa. ARP-sanoman sisältönä on ”who has 192.168.255.20 tell 192.168.255.10”, missä 192.168.255.10 on koneen A IP-osoite. Ethernet-verkossa kulkeva sanoma sisältää lähettäjän MAC-osoitteen,

jolloin kone B kykenee vastaamaan kuvion 5 oikean puolen mukaisesti suoraan koneelle A ”192.168.255.20 is at 00:11:22:33:44:55”, missä 00:11:22:33:44:55 on koneen B verkkokortin MAC-osoite. Saatuaan vastauksen kone A tallentaa tiedon ARP välimuistiin, jotta jokaista lähetettävää IP-pakettia varten ei tarvitse kysyä MAC-osoitetta uudelleen. Tiedon säilytysaika välimuistissa vaihtelee laitteen käyttöjärjestelmien välillä. Esimerkiksi Linuxissa keskimääräinen oletussäilytysaika on yksi minuutti, Windowsissa kaksi minuuttia ja Ciscon reitittimissä neljä tuntia. (RFC826 1982.)



KUVIO 5. ARP-protokollan toiminta.

Jotta kytkentäisessä verkossa kyettäisiin seuraamaan kahden laitteen välistä liikennettä, tarvitsee verkkoon kytkettyjen laitteiden reititystauluja päästä muokkaamaan, jotta liikenne reitittyisi liikennettä kuuntelevalle laitteelle. Tämä toteutetaan lähettämällä tarkoituksellisesti verkkoon virheellisiä ARP-sanomia, tätä tekniikkaa kutsutaan ARP-huijaukseksi (ARP Spoofing). ARP-huijauksessa hyökkäyksessä käytettävältä työasemalta lähetetään hyökkäyksen kohteena olevien laitteiden ARP-sanomiin valheellisia vastauksia. Tällöin saadaan laitteiden välinen liikenne kulkemaan hyökkäävälle työasemalle vastapään laitteen sijaan. Hyökkäävä työasema puolestaan välittää liikenteen edelleen oikealle vastaanottajalle. Hyökkääjä voi tällöin joko tyytyä seuraamaan laitteiden välistä

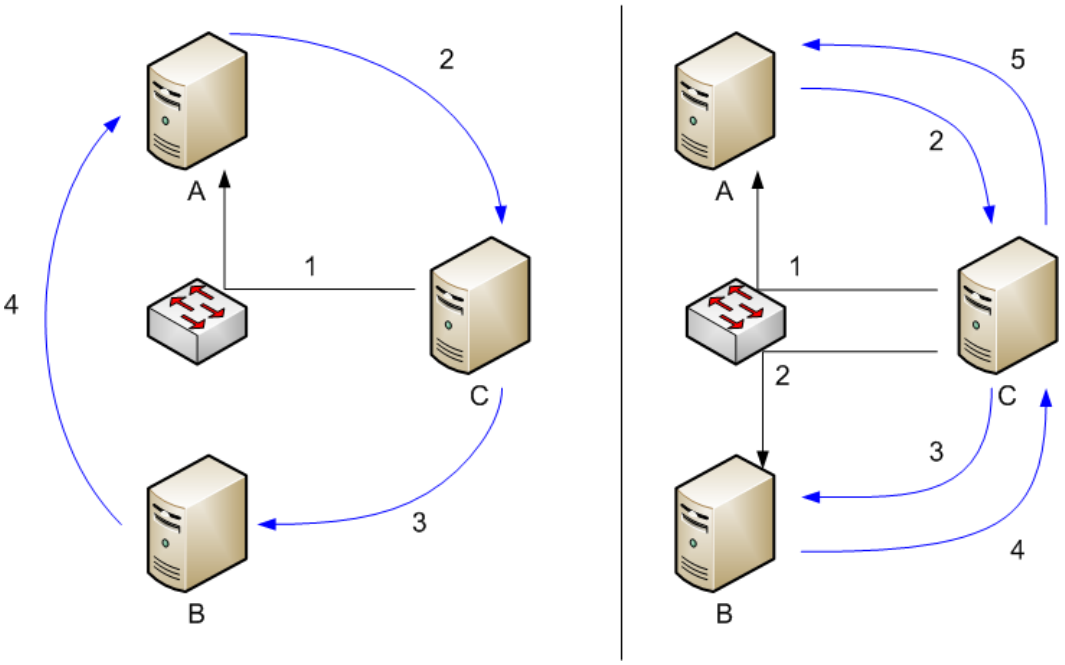
liikennettä tai muokata liikennettä ennen sen välittämistä edelleen. Hyökkääjä voi myös tuhota vastaanottamansa paketit lähettämättä niitä edelleen oikealle vastaanottajalle, jolloin suoritetaan palvelunestohyökkäys. (Porter 2006, 251-255; VOIPSA Threat Taxonomy Wiki 2006.)

Suuressa osassa käyttöjärjestelmä ARP-protokolla on toteutettu tilattomana protokollana, jolloin lähetettyyn kyselyyn ei jäädä odottamaan vastausta verkosta vaan laitteen vastaanotettua ARP-vastauspaketin, tämä päivittää ARP-välimuistinsa vastauspaketin osoittamalla tiedolla. Tämä tekee ARP-protokollan haavoittuvaksi niin sanottua ARP-välimuistin myrkytyshyökkäystä (ARP cache poisoning) vastaan. Tällöin hyökkääjän ei tarvitse odottaa, kunnes kohde lähettää verkkoon kyselyn halutulle päätelaitteelle ARP-kyselyn ja kilpailla oikean päälaitteen kanssa ARP-vastauksen lähettämisestä, vaan tämä voi luoda virheellisiä ARP-vastauspaketteja ja lähettää niitä kohdelaitteelle sopivin väliajoin, jolloin kohdelaite päivittää ARP välimuistiinsa todellisen päätelaitteen IP-osoitteelle oikean MAC-osoitteen sijaan hyökkääjään MAC-osoitteen. Lähettämällä näitä riittävän usein, ei hyökkäyksen kohde lähetä verkkoon ollenkaan ARP-kyselyitä kohteen IP-osoitteen selvittämiseksi, jolloin tämä voisin ”vahingossa” saada päätelaitteen todellisen MAC-osoitteen selville. (Porter 2006, 251-255; VOIPSA Threat Taxonomy Wiki 2006.)

Kuvion 6 vasemmassa puoliskossa esitetään kuinka hyökkäävä kone C lähettää koneelle A väärennettyjä ARP-vastaussanomia (1), jonka seurauksena tämä lähettää laitteelle B tarkoitetut IP-paketit hyökkäävälle koneelle C (2). Hyökkääjä puolestaan välittää paketit edelleen oikealle vastaanottajalle eli koneelle B (3), jolloin koneiden A ja B välinen yhteys toimii kuten normaalisti. Koneen B vastatessa koneelle A tämä tekee myös ARP-kyselyn, johon tämä saa vastaukseksi koneen A MAC-osoitteen. Tällöin B:n vastauspaketit A:lle kulkevat suoraan oikealle vastaanottajalle.

Mikäli hyökkääjä haluaa seurata myös koneen B lähettämiä sanomia A:lle, täytyy tämän tehdä samanlainen hyökkäys konetta B vastaan, jolla tämä saa syötettyä B:n ARP välimuistiin oman MAC osoitteensa koneen A IP-osoitetta vastaavaksi. Tällainen tilanne on esitetty kuvion 6 oikeassa puoliskossa. Hyökkääjä lähettää

sekä A että B koneille väärennettyjä ARP-sanomia ARP välimuistin vääristämiseksi (1 ja 2). Tällöin A:n B:lle lähettämät paketit (2) kulkevat hyökkääjälle, joka välittää ne edelleen B:lle (3) yhteyden toimimiseksi. Kun B vastaa A:lle, se lähettää paketit ARP välimuistissaan olevalle MAC osoitteelle, joka myös osoittaa hyökkääjään (4). Hyökkääjä välittää jälleen paketit edelleen A:lle (5).



KUVIO 6. ARP-protokollaan kohdistuvat hyökkäykset

Kun hyökkääjä pystyy kaappaamaan VoIP-liikenteen päätelaitteiden väliltä, pystyy tämä tallentamaan myöhempää käyttöä varten kaiken päätelaitteiden välillä siirtyneen tiedon, niin puhelun sisällön kuin signaloinnin sekä laskutuksellisen tiedon ja mahdolliset salasanat ja pin-koodit. Sen lisäksi, että hyökkääjä tyytyy vain seuraamaan ja mahdollisesti myös vaikuttamaan kaappaamaansa liikenteeseen, voi tämä myös esittää olevansa vaikkapa toinen päätelaite tai yhdyskäytävä. (Porter 2006, 251-255; VOIPSA Threat Taxonomy Wiki 2006.)

ARP-huijauksia voidaan havainnoida verkosta työkalulla, joka seuraa verkossa liikkuvia ARP-sanomia ja vertailemalla niissä ilmoitettavia MAC- ja IP –pareja. Mikäli samalle IP-osoitteelle ilmoitetaan useampia MAC-osoitteita tai jonkin IP-

osoitteen käyttämä MAC-osoite muuttuu ilman syytä, on syytä tarkastaa sanomien oikeellisuus ja lähde. ARP huijauksia voidaan estää luomalla verkon aktiivilaitteisiin kiinteät ARP-osoitetaulut. Tämä on ylläpidollisesti erittäin työlästä, varsikin vähänkään suuremmissa verkkoympäristöissä. (Porter 2006, 251-255; VOIPSA Threat Taxonomy Wiki 2006.)

3.2 Suojautuminen

Salaamalla päätelaitteiden välinen liikenne voidaan huomattavasti hankaloittaa liikenteen sisällön seurantaa. Vahvasti salatun liikenteen murtaminen vie paljon aikaa, jolloin murretun istunnon sisällöllä ei välttämättä ole enää arvoa hyökkääjälle. Liikenteen salaaminen voidaan suorittaa eri tavoin riippuen käytetystä VoIP-tekniikasta. H.323 –liikenteen salaamiseen käytetään H.235.x –salausprotokollia, kun taas SIP-liikenteen kanssa käytetään TLS (Transport Layer Security), S/MIME (Secure/Multipurpose Internet Mail Extensions) ja SRTP (Secure Real-Time Transport Protocol)-protokollia. (Porter 2006, 417-419; RFC2246 1999.)

TLS (Transport Layer Security), joka pohjautuu SSL (Secure Sockets Layer)-protokollaan, on määritelty IETF:n dokumentissä RFC 2246. Alkuperästään huolimatta ei ole yhteen sopiva SSL-protokollan kanssa. Protokollan tehtävänä on salata kahden pisteen välinen yhteys samalla varmistaen siirretyn tiedon eheys ja tunnistaa yhteyden osapuolet näiden käyttämien X.509 sertifikaattien perusteella. TLS-protokolla muodostuu kahdesta kerroksesta, TLS Record -protokolla- sekä TLS Handshake -protokollakerroksesta. TLS on täysin riippumaton sen päällä kuljetettavasta sovellusprotokollasta. Näin ollen sitä voidaan hyödyntää periaatteessa minkä tahansa protokollan, kuten SIP, yhteydessä liikenteen salaamiseksi. (Porter 2006, 417-419; RFC2246 1999.)

Alimmaisen kerroksena toimii TLS Record protokollakerros, joka hyödyntää tiedonsiirrossa luotettavaa siirtokerroksen protokollaa, yleisimmin TCP:tä. TLS Record protokolla tarjoaa yhteyden turvallisuuden kaksi perusominaisuutta, yhteyden yksityisyyden ja luotettavuuden. Yhteyden yksityisyyttä varten yhteys

salataan symmetrisellä salauksella (esim, DES (Data Encryption Standard) tai RC4 (Rivest Cipher 4)). Jokaista yhteyttä varten luodaan oma yksilölliset salausavaimet, mutta TLS Record protokollaa voidaan käyttää myös ilman liikenteen salausta. Yhteyden luotettavuus varmistetaan lisäämällä jokaiseen siirrettyyn sanomaan tarkastussumma, jonka perusteella voidaan varmistua sanoman eheydestä lähettäjän ja vastaanottajan välillä. TLS Record protokollaa käytetään ylempien protokollakerrosten siirtämiseen. TLS Handshake protokolla siirretään käyttäen TLS Record protokollaa. (RFC2246 1999.)

TLS Handshake protokollaa käytetään yhteyden päätepisteiden tunnistamiseen sekä salausalgoritmien ja salausavainten valintaan päätteiden välillä ennen varsinaisen sovellusliikenteen aloittamista. TLS Handshake protokolla tarjoaa yhteyden turvallisuutta varten kolme toiminnallisuutta, osapuolien tunnistus, salausavainten neuvottelu ja valinnan luotettavuuden takaaminen. Osapuolien tunnistus tapahtuu käyttämällä asymmetrista tai julkiseen avaimeen perustuvaa salausta kuten RSA (Rivest Shamir Adleman) tai DES. Salausavainten luotettava neuvottelu takaa sen, että ulkopuoliset eivät pääse käsiksi valittuun avaimeen vaikka pystyisivät seuraamaan liikennettä. Luotettavuus tulee siitä, että ulkopuoliset eivät pysty vaikuttamaan avaimen valintaprosessiin ilman, että neuvottelevat osapuolet sen huomaavat. (RFC2246 1999.)

SRTP (Secure Real-Time Transport Protocol) määrittelee RTP-protokollan suojaamisen käytetyt menetelmät. SRTP huolehtii RTP-liikenteen salaamisesta, eheydestä ja suojaamisen toistohyökkäystä vastaan. Liikenne salataan AES-algoritmilla. Oletuksena salauksessa käytetään 128 bittistä salausavainta liikenteen salaamiseen. Liikenteen eheys varmistetaan laskemalla sanomasta HMAC-SHA1 (Hash Message Authentication Code – Secure Hashing Algorithm 1) –algoritmilla sanoman otsikkotiedoista ja sisällöstä 160 bittinen tarkastussumma, joka lisätään lähetettävään sanomaan. Tarkastussumman laskennassa käytetään salaista avainta, jolloin varmistetaan, että salausavainta tuntematon ei pysty muokkaamaan sanomaa huomaamatta. Tämä myös estää sanoman uudelleenkäyttämisen niin sanotussa toistohyökkäyksessä, jolloin hyökkääjä ei voi käyttää keräämiään sanomia myöhemmin hyökkäyksen apuna. (Porter 2006, 420-421; RFC3711 2004.)

Pelkän VoIP-liikenteen salaamisen sijaan voidaan kaikki päätelaitteen ja yhdyskäytävän välinen liikenne salata käyttämällä VPN-tekniikkaa (Virtual Private Network), jolloin päätelaitteen ja yhdyskäytävän välille muodostetaan oma, suojattu verkkoyhteys. Tämä on kuitenkin huomattavasti vaativampi toimenpide sekä ylläpidollisesti että päätelaitteelta vaadittavan laskentakapasiteetin suhteen, eikä se siten välttämättä sovellu kaikkiin tilanteisiin. Varsinkin kevyissä päätelaitteissa yleensä laskentakapasiteetti on hyvin pieni, jolloin vaativampi laskentakapasiteetin käyttö lisää laitteen virrankulutusta ja lyhentää käyttöaikaa.

Vaikka päätelaitteiden välisessä liikenteessä käytetään vahvaa salausta, mutta ei molemminpuolista vahvaa tunnistautumista, voi hyökkääjä esittää yhdyskäytävää molemmille laitteille, jolloin liikenne kulkee salattuna päätelaitteiden ja hyökkääjän välillä ja hyökkääjä saa liikenteen helposti purettua. Käytettäessä vahvaa tunnistautumista, myös hyökkääjän on kyettävä tunnistautumaan päätelaitteelle. Mikäli hyökkääjällä ei ole käytettävissään oikealle yhdyskäytävälle tai päätelaitteelle kuuluvia tunnisteita, huomaavat muut verkon käyttäjät yhdyskäytävän vaihtuneen ja ilmoittaa tästä ylläpidolle. (VOIPSA Threat Taxonomy Wiki 2006.)

Tietoliikenteen tietoturvaa voidaan lisätä erottelemalla samassa fyysisessä verkossa kulkeva liikenne useampaan loogiseen verkkoon VLAN-tekniikalla (Virtual Local Area Network). VLAN on IEEE (Institute of Electrical and Electronics Engineers):n määrittelemä 802.1q-standardi, jolla voidaan eriyttää verkossa kulkeva liikenne useampaan eriytettyyn virtuaaliseen lähiverkkoon, joiden liikenne kulkee täysin erillään toisistaan. Tällöin verkkojen välistä liikennettä voidaan kontrolloida tarkasti tai estää se kokonaan, jolloin VoIP-liikennettä kuljettavaan VLAN:iin ei voida vaikuttaa muuta dataliikennettä kuljettavasta VLAN:ista käsin, eivätkä toisen VLAN:in ongelmat vaikuta toisen VLAN:in liikenteeseen. (Porter 2006, 375-376).

VLAN:it voidaan määritellä joko staattisesti tai dynaamisesti kytkimiin. Staattisessa konfiguraatiossa kytkimen portit määritellään kuuluvaksi tiettyyn VLAN:iin. Kun laite kytketään tähän porttiin, se liikennöi automaattisesti siinä

VLAN-verkossa, johon kyseinen kytkimen portti on määritelty kuuluvaksi. Kun laite siirretään verkossa toiseen kytkinporttiin, joudutaan tämä uusi portti määrittelemään kuuluvaksi samaan VLANiin, johon laite oli alun perin kytkettynä mikäli halutaan säilyttää alkuperäinen verkkoyhteys. (Wikipedia 2007.)

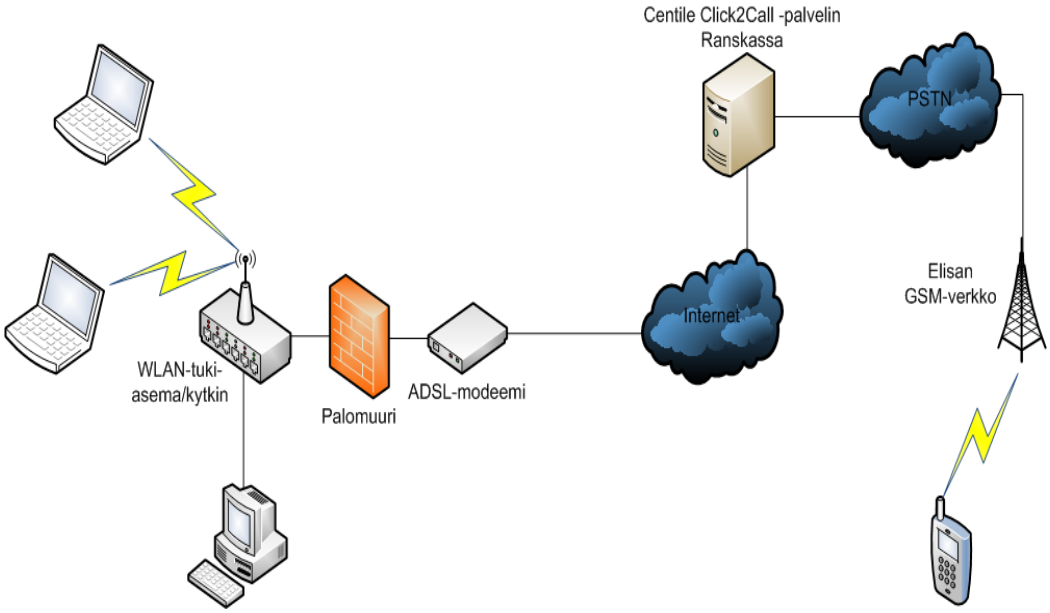
Dynaamisesti määritellyissä VLAN:eissa laitteen MAC-osoitteen tai 802.11x-autentikoinnnin perusteella päätetään, mihin VLAN-verkkoon laite liitetään, kun se kytketään lähiverkkoon. Kytkinten välillä usean VLAN:in liikenne voidaan siirtää yhtä fyysistä yhteyttä pitkin lisäämällä Ethernet-kehykseen tieto siitä, mihin VLAN:iin se kuuluu. Tällaista kytkimen tai reitittimen porttia, joka kuljettaa usean VLAN:in liikennettä, kutsutaan yleisesti trunkiksi (trunk), kun taas laitevalmistaja Cisco käyttää tästä nimitystä kanava (channel). (Wikipedia 2007.)

3.3 Muut riskit

Hyökkäykset voivat kohdistua verkon lisäksi myös päätelaitteiden tai palvelimien sovelluskoodissa tai käyttöjärjestelmässä oleviin haavoittuvuuksiin sekä virheelliseen tai puutteelliseen konfigurointiin. Päätelaitteiden sovelluskoodissa olevia haavoittuvuuksia hyödyntämällä voi hyökkääjä kyetä tekemään palvelunestohyökkäyksen päätelaitteita vastaan. Eräs tällainen käyttöjärjestelmän haavoittuvuuksia hyödyntävä hyökkäys on suurten pakettien lähettäminen päätelaitteelle. Eräissä VoIP-puhelinlaitteissa on esiintynyt haavoittuvuus, jolla puhelin saadaan jumiutettua lähettämällä tälle UDP-paketti, joka on suurempi kuin 65534 tavua (Porter 2006, 242-248.)

Puutteellinen tai virheellinen konfiguraatio puolestaan saattaa helpottaa hyökkääjän työtä, joko paljastamalla järjestelmän toimintaan liittyviä parametreja tai heikentämällä tai kokonaan poistamalla käytöstä verkosta salaukseen ja tunnistukseen liittyviä tekijöitä, jolloin hyökkääjän ei tarvitse tehdä niin paljoa työtä saavuttaakseen tavoitteensa.

4 TESTAUS



KUVIO 7. Kaaviokuva testausjärjestelystä.

Kuviossa 7 kuvattu verkko toimii seuraavasti: kannettavat tietokoneet ovat yhteydessä langattomaan tukiasemaan ja pöytäkone suoraan Ethernet-kaapelilla kytkimeen. Kyseessä on verkko, jossa on käytössä osoitteenmuunnos ja jossa yhteys kulkee kytkimen, palomuurin ja ADSL (Asymmetric Digital Subscriber Line) -modeemin kautta internetiin.

Verkkokokoonpanoon kuului ADSL-modeemi Nokia M1122, Linux rautapalomuuri, Linksysin langaton tukiasema kannettaville ja Ethernet kaapeli pöytäkoneeseen.

Testilaitteistossa oli käytössä kannettavat tietokoneet IBM Thinkpad 600, HP dv4057EA sekä Dell latitude D820. Lisäksi testauksissa käytettiin pöytäkonetta AMD Athlon XP 2800 + 2,08GHz prosessorilla.

Testaus tapahtui Centilen Click-To-Call –demojärjestelmää käyttäen. Palvelu toimii Flash-pohjaisesti. Järjestelmässä käytettiin Centilen omaa Ranskassa sijaitsevaa palvelinta.

Testaus tapahtui Centilen internetsivustolla sijaitsevan demoympäristön kautta, joka on luotu vain demokäyttöön ja testaamiseen. Kirjautumalla sisään järjestelmään annetuilla tunnuksilla pääsi ikkunaan, johon syötettiin puhelinnumero muodossa 000358+puhelinnumero ilman ensimmäistä nollaa. Tämän jälkeen puhelu muodostui mikrofonin sallimiskyselyn ja puhelun muodostamisvarmistuksen jälkeen haluttuun numeroon. Testaukset suoritettiin soittamalla muutamiin eri GSM numeroihin ja omien havaintojen perusteella määriteltyihin tuloksiin perustuen teimme analysoinnin äänen laadusta sekä viiveistä. Mitään virallista mittaria äänen laadusta tai viiveiden pituudesta ei ollut käytettävissä.

Click-To-Call –palvelu itsessään toimii siten, että palveluntarjoajan internet-sivustolla sijaitsee linkki, jonka aktivoimalla järjestelmä muodostaa yhteyden VoIP:in kautta valmiiksi linkkiin määriteltyyn numeroon.

Linkin aktivoinnin jälkeen järjestelmä kysyy tarvittavat tiedot, mikrofonin sallimisen, ääni-asetukset sekä puhelun yhdistämisen sallimisen. Tämän jälkeen puhelu yhdistyy palvelun osoittamaan paikkaan.

4.1 Click-To-Call

Click-To-Call viittaa prosessiin, jossa web-pohjainen liikenne muunnetaan puheluksi loppukäyttäjän ja jonkin toisen osapuolen välillä. (Wikipedia 2007.)

Click-To-Call prosessit vaihtelevat alustasta riippuen, mutta ne voidaan jakaa kahteen eri pääryhmään: Ensimmäisessä tietokone hoitaa yhteyden muodostamisen (yleisimmin VoIP:ia käyttäen), ja toinen on ns. takaisinsoitto, jossa käyttäjä antaa järjestelmälle puhelinnumeronsa ja välitysjärjestelmä muodostaa puhelun käyttäjän ja toisen osapuolen välille. Tällainen takaisinsoitto-palvelu on enemmänkin automaattinen numeronvalintajärjestelmä kuin varsinainen Click-To-Call –järjestelmä. (Wikipedia 2007.)

Kun käyttäjä selailee sivustoa matkapuhelinta käyttäen, Click-To-Call toimii nimensä mukaisesti. Puhelinnumerot toimivat linkkeinä kuten normaalit hyperlinkit, jolloin numeroa klikkaamalla puhelin soittaa tähän numeroon. (Wikipedia 2007.)

Yksi Click-To-Call:in merkittävimmistä hyödyistä palveluntarjoajalle on, että se helpottaa yritysten asiakkaiden seurantaa, kun nämä siirtyvät internetsivustolta tilaamaan tuotteita puhelimitse. Click-To-Call:ia voidaan hyödyntää myös mainostamisessa. Tällöin tuotteista kiinnostuneet voivat klikata mainoksessa olevaa puhelinnumeroa tai siihen upotettua painiketta, jolloin he voivat soittaa kyseisen mainoksen edustajalle. (Wikipedia 2007.)

Google on kokeillut Click-To-Call:in takaisinsoitto palveluita Google Maps tuotteessaan, mutta luopunut tästä myöhemmin. Lokakuussa 2007 Google on luvannut lisätä Click-To-Call toiminnallisuuden osana Google Adwords mainostuotettaan. (Wikipedia 2007.)

4.2 Centile Click-To-Call

Click-To-Call –järjestelmä pohjautuu Java-pohjaiseen palvelimeen. Käyttäjälle päin järjestelmä näkyy flash-sovelluksena, joten käyttäjän koneeseen ei tarvitse asentaa mitään selainkohtaista liitännäistä eikä muuta erillistä asiakassovellusta. Flash-sovellus käyttää RTMP (Real Time Messaging protocol) –protokollaa siirtääkseen ääntä käyttäjän flash-sovelluksen ja Centilen palvelimen välillä.

RTMP on Adoben kehittämä protokolla äänen, videon ja datan reaaliaikaiseen siirtämiseen internetin yli flash-sovelluksen ja palvelimen välillä.

Järjestelmästään Centile ei halua luovuttaa tarkempia tietoja julkisuuteen. Lopullinen palvelu tullaan toteuttamaan suljetussa Elisan yritysverkossa. Järjestelmän tietoturvaan on kiinnitetty huomiota suunnittelun ja toteutuksen yhteydessä ja se on auditoitu mm. Elisan tietoturvaryhmän toimesta. Elisa tulee tuotteistamaan Click-To-Call –palvelun osana Elisa ContactCenter -palvelutuotetta Elisa Asiakaspalveluratkaisuissa osana monikanavaisuutta vuoden 2008 puolella.

4.3 Flash

Adobe Flash on suosittu teknologia, jolla voidaan lisätä animaatiota, videota ja muita interaktiivisia sovelluksia websivustoille. Flash-sovelluksia voidaan toistaa useilla eri sovelluksilla ja laitteilla. Flash tukee vektori- ja rasterigrafiikkaa, ActionScript -komentokieltä sekä äänen ja videon kaksisuuntaista siirtoa. (Wikipedia 2007.)

Flash pohjautuu FutureWave Software nimisen yrityksen vuonna 1993 tekemään SmartSketch piirrustustyökaluun. Internetin suosion noustessa FutureWave Software ymmärsi sovelluksensa kehitysmahdollisuudet vektoripohjaisen web-animaatiotyökaluna. Vuonna 1995 julkaistiin uusi versio nimellä FutureSplash Animator, johon oli lisätty animointitoiminto. Joulukuussa 1996 Macromedia osti FutureWavelta tämän sovelluksen ja julkaisi sen nimellä Flash. Joulukuussa 2005 Adobe osti Macromedian ja lisäsi tämän tuotteet omaan tarjontaansa. (Wikipedia 2007.)

Adobe Flash jakautuu kahteen osaan: Adobe Flash Professional kehitystyökaluun Flash-sovellusten tekemiseen sekä Adobe Flash Player sovellukseen, jolla voidaan toistaa Flash-sovelluksia. Flash-sovelluksien tekoon on julkaistu myös avoimeen lähdekoodiin perustuvia sovelluksia, mutta näiden toimivuus ei yllä vielä lähellekään Adoben sovelluksen toiminnallisuuksia. (Wikipedia 2007.)

4.4 Tulokset

TAULUKKO 1. Tulosten yhteenveto

		Internet Explorer	Mozilla Firefox	Opera
Pöytäkone	Win98SE	EI TOIMI	EI TOIMI	EI TOIMI
Pöytäkone	Win2000	TOIMII	TOIMII	TOIMII
Pöytäkone	Win XP	TOIMII	TOIMII	TOIMII
Kannettava ThinkPad 600	Win98SE	TOIMII	TOIMII	TOIMII
Kannettava ThinkPad 600	Win2000	TOIMII	TOIMII	TOIMII
Kannettava HP Pavilion	Win XP	TOIMII	TOIMII	TOIMII
Kannettava Dell latitude	Win Vista	TOIMII	TOIMII	TOIMII

Taulukossa 1 on vihreällä yhdistelmät, jotka toimivat moitteettomasti. Punaisella merkittynä yhdistelmät, jotka eivät toimineet ollenkaan. Keltaisella mainittuna yhdistelmä jossa Windows 98SE kannettava antoi Adobe Flash Playerin hitaudesta johtuvan virheilmoituksen, mutta Clikc-To-Call palvelu toimi kuitenkin siitä huolimatta normaalisti.

4.5 Käytettävyys

Flashin puuttuminen koneesta saattaa aiheuttaa ongelmia käyttäjille. Sen asentaminen saattaa kestää koneesta riippuen muutamasta minuutista jopa yli puoleen tuntiin. Flashin asentaminen saattaa olla ongelmallinen, sillä kaikilla käyttöjärjestelmillä ja selaimilla palvelu ei asennu automaattisesti, vaikka selain näin ilmoittaisikin. Tällöin käyttäjän on haettava se valmistajan sivuilta ja asennettava se manuaalisesti ohjeiden mukaisesti. Lisäksi käyttäjällä pitää olla oikeudet asentaa koneeseen sovelluksia.

Flashin käsin asentaminen ei myöskään aina onnistu, vaan esimerkiksi eräässä testikoneessa todettiin ensin, että sovellus on asennettuna koneeseen, mutta se ei toiminut. Tämän jälkeen yritettiin päivittää uudempaa versiota valmistajan sivustolta, josta saatiin ilmoitus että koneessa on jo asennettu versio, eikä päivittäminen onnistunut useasta yrityksestä huolimatta. Tällöin ohjelma jouduttiin poistamaan koneesta käsin Adoben-sivustolta löydetyn ohjeen perusteella poistamalla Windowsin rekisteristä määritellyt rekisteriavaimet sekä poistamalla Windowsin järjestelmähakemistoista Flash Playeriin liittyvät tiedostot. Näiden toimenpiteiden ja uudelleenkäynnistyksen jälkeen uudempi versio Flash Playerista pystyttiin asentamaan koneeseen.

Mikäli sovelluksen mikserin asetuksissa ei ole mikrofonin äänen toistoa vaimennettu, kuuluu kaiuttimista mikrofoniin puhuttu ääni. Tavallista headsetia käytettäessä aiheuttaa sen, että kuulokkeista kuuluu oma ääni, joka ainakin alkuun kuulostaa häiritsevältä, mutta tämän kanssa tulee toimeen. Käytettäessä avoimia kaiuttimia ja mikrofonia tai kannettavan integroitua mikrofonia ja kaiuttimia ääni rupeaa kiertämään, jolloin palvelun käytettävyys heikkenee huomattavasti, koska tällöin puheesta ei saa mitään selvää.

Ensimmäistä kertaa palvelua käytettäessä tulee käyttäjän hyväksyä erilaisia kohtia palvelun asetuksista. Mikäli koneessa on useampia eri audiolaitteita, pitää käyttäjän osata valita oikeat laitteet sekä Windowsin valikoista että Flash Playerin asetuksista. Oletuksena ei todennäköisestikään ole valittuna oikeita laitteita, vaan käyttäjän pitää tietää mitä tekee. Lisäksi valintakohdat ovat pieniä sekä esitetty

ainoastaan kuvallisilla symboleilla, jolloin vanhemmilla käyttäjillä on varmastikin ongelmia näitä valitessaan.

4.6 Tietoliikenne

Tietoliikenneyhteytenä toimi Elisan ADSL-yhteys 8M/1M. Järjestelmän toimivuutta testattiin myös yhteysnopeutta hidastamalla porrastetusti palomuurista käsin, ja palvelu toimi nopeudesta riippumatta hyvin. Viive puheen siirrossa kasvoi yhteysnopeuden hidastuessa, mutta 16k nopeudella puhelua ei enää onnistuttu muodostamaan.

Kun palvelu toteutetaan yrityksen lähiverkkoon, on erittäin epätodennäköistä, että järjestelmän käyttöön ei riittäisi tarpeeksi tietoliikennekapasiteettia. Tällöin myös yhteyteen kohdistuvat tietoturvauhat ovat lähes olemattomat, sillä tällaisissa ympäristöissä tietoturva on otettu huomioon tarkasti suunnitteluvaiheesta lähtien.

5 YHTEENVETO

5.1 Keskeiset tulokset

Tietoliikenne nopeus ei aiheuta huomattavia eroja palvelun käytettävyyteen. Puhelun muodostamisen viive vain kasvaa yhteysnopeuden hidastuessa. Äänen laadussa ei huomattavia eroja, pätkintä tosin lisääntyy hieman hitaammalla yhteydellä. 16kbps:n nopeudella yhteys ei enää muodostunut.

Palvelu toimii todennäköisesti kaikilla laajakaistaliittymillä, ISDN- ja jopa modeemiyhteyksillä. Myös 3G-verkossa UMTS (Universal Mobile Telecommunications System) -yhteys riittää, GPRS (General Packet Radio Service) -yhteys on todennäköisesti liian hidas palvelun käyttämiseen, mutta pakettiverkon latenssi saattaa aiheuttaa ongelmia kummassakin tapauksessa.

Headsetillä on vaikutusta äänenlaatuun ja linjalla esiintyviin häiriöihin, mutta headsetin olemassaolo on tärkein tekijä palvelun käytettävyyden kannalta. Koneen oma mikrofoni ja kaiuttimet tai irralliset kaiuttimet ja mikrofoni saavat äänen kiertämään herkästi, jolloin palvelun käytettävyys varsinkin asiakaspalvelijan näkökulmasta on erittäin huono.

Plantronicsin DSP-100 aiheutti vastaanottavaan päähän jatkuvan taustahäiriön, ja silloin kun headsetiin ei puhuttu, alkoi kuulua rutinaa ja suhinaa, joka poistui, kun headsetin mikrofoniin puhuttiin. Headsetin ääni oli myös hyvin metallinen. Plantronicsin headset on hyvin herkkä ulkoisille häiriölähteille, ja laitteen pitkät johdot toimivat antennina ja vastaanottavat häiriöitä tehokkaasti.

Tietokoneen suorituskyvyllä ei niinkään ole merkitystä palvelun toimivuuden kannalta. Hitaimmalla testikoneella (P2 300MHz) sovellus antoi varoituksen mahdollisesta suorituskyky ongelmasta, mutta tästä huolimatta palvelun toimivuudessa ei havaittu eroa nopeampiin koneisiin nähden.

5.2 Jatkotoimenpiteet ja tulevaisuus

Palvelua voitaisiin käyttää tulevaisuudessa esimerkiksi myynnin tai asiakaspalvelun apuna. Palveluntarjoajan Internetsivustolla asiakas voisi esimerkiksi tilausta tai muuta kaavaketta täyttäessään ja ongelmatapauksen sattuessa klikata sivustolla olevaa linkkiä, joka ottaisi yhteyden Click-To-Call -palvelua käyttäen palveluntarjoajaan, joka pystyisi auttamaan ongelmassa reaaliaikaisesti. Palvelun tuottamisessa on kuitenkin huomioitava sen käyttöönottamiseen liittyvät ongelmat. Mikäli järjestelmä on liian hankala käyttää tai sen käytön aloittaminen on ongelmallista suurimmalle osalle asiakkaista, tulisi tuotteen käyttöönottamista harkita uudelleen, sillä se saattaa aiheuttaa enemmän negatiivista mielikuvaa yrityksestä kuin tuoda lisäarvoa asiakkaille.

Palvelu toimii valveutuneimmilla käyttäjillä varmasti hyvinkin, mutta vanhemmilla ja ei niin teknisillä henkilöillä palvelun käytössä tulee todennäköisesti hurjasti ongelmia. Kyseistä palvelua ei saada toimimaan helposti ja yksinkertaisesti ilman käyttäjän omaa teknistä osaamista ja asetusten hallitsemista.

Yrityksien käytössä palvelun käyttö saattaisi myös olla ongelmallinen sen vuoksi, että usein yrityksen henkilöstön käytössä olevat tietokoneet ovat jonkin ulkoisen yrityksen tai yrityksen oman mikrotuen hallinnoimia. Tällöin käyttäjillä ei ole järjestelmän ylläpito-oikeuksia koneilleen, eivätkä näin ollen kykene tekemään suuria muutoksia asetuksiin. He eivät myöskään pysty asentamaan koneilleen uusia sovelluksia, jolloin ongelmia tulee myös Flash Playerin asennuksessa, mikäli koneille ei ole asennettu sitä jo alunperin.

Käyttäjien ongelmana tulee olemaan myös ulkoiset kaiuttimet ja mikrofonit, joiden kautta puhuttaessa ääni kiertää pienimmilläkin äänenvoimakkuuksilla. Ainoa toimiva ratkaisu palvelun käyttöön on headset, vaikka niissäkin on toiminnaltaan monenlaisia laitteita. Pitkillä johdoilla varustetut headsetit toimivat suurina häiriölähteinä palvelussa, jolloin äänihäiriöt kasvavat radikaalisti.

Click-To-Call –palvelussa pitäisi ottaa huomioon sen helppo käytettävyys. Lisäksi palvelussa pitäisi erehtymisen mahdollisuudet karsia pois. Click-To-Call:in mahdollisimman helppo käytettävyys taattaisiin sillä, että valintakohdat asetuksissa olisivat mahdollisimman karsittuja ja huomiota herättäviä sekä selkeitä.

Palvelun toimivuutta voisi testata myös muilla kuin Windows-käyttöjärjestelmillä. Tämän työn puitteissa ei muita käyttöjärjestelmiä testattu työn tilaajan rajauksen vuoksi. Vaikka suurin osa käyttäjäkunnasta käyttääkin Windows-käyttöjärjestelmien eri versioita, on esimerkiksi Linux-käyttöjärjestelmän suosio kasvussa, minkä vuoksi on entistä todennäköisempää, että palvelua tultaisiin käyttämään myös tällaiselta koneelta. Periaatteessa Flashilla toteutettujen sovellusten pitäisi olla käyttöjärjestelmä riippumattomia, saattaa sen toteutuksessa silti olla poikkeuksia, kuten testeissä huomattiin jo eri Windows versioiden välillä.

Tulevaisuudessa on todennäköistä, että VoIP tulee syrjäyttämään suurelta osin normaalin lankaverkon sekä siirtämään osan matkapuhelinverkon liikenteestä tietoverkkoihin. Nykyiset 3G-verkot hyödyntävät jo VoIP:ia puheensiirrossa, joten on luonnollista, että tämä suuntaus leviää myös kiinteän verkon puolelle syrjäyttäen vanhaa piirikytkentäistä teknologiaa.

LÄHTEET

Baugher, M., McGrev, D., Naslund, M., Carrara, E., Norrman, K. 2004. The Secure Real-time Transport Protocol (SRTP) [verkkojulkaisu]. Internet Engineering Task Force [viitattu 3.11.2007]. Saatavissa: http://www.ietf.org/rfc/rfc3711.txt.

Dierks, T., Allen, C. 1999. The TLS Protocol [verkkojulkaisu]. Internet Engineering Task Force [viitattu 2.11.2007]. Saatavissa: http://www.ietf.org/rfc/rfc2246.txt.

Groves, C., Pantaleo, M., Anderson, T., Taylor, T. 2003. Gateway Control Protocol Version 1 [verkkojulkaisu]. Internet Engineering Task Force [viitattu 31.10.2007]. Saatavissa: http://www.rfc-editor.org/rfc/rfc3525.txt.

Handley, M., Jacobson, V., Perkins, C. 2006. SDP: Session Description Protocol [verkkojulkaisu]. Internet Engineering Task Force [viitattu 12.11.2007]. Saatavissa: http://www.ietf.org/rfc/rfc4566.txt.

Handley, M., Schooler, E. 1996. Session Initiation Protocol [verkkojulkaisu]. Internet Engineering Task Force [viitattu 30.10.2007]. Saatavissa: http://www.cs.columbia.edu/sip/drafts/mmusic/draft-ietf-mmusic-sip-00.pdf.

Lintula, P. 2004. Suoraviestintää ja läsnäoloa SIP:illä. Tampere: Tampereen Yliopisto

Plummer, D. 1982. An Ethernet Address Resolution Protocol [verkkojulkaisu]. Internet Engineering Task Force [viitattu 1.11.2007]. Saatavissa: http://www.faqs.org/rfcs/rfc826.html.

Porter, T., Kanclirz, J., Zmolek, A., Rosela, A., Cross, M., Chaffin, L., Baskin, B. & Shim, C. 2006. Practical VoIP Security. Rockland, MA, USA: Syngress Publishing, Inc.

Radvision. 2005. Session Initiation Protocol – Technical Overview. Radvision.

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley M., Schooler, E. 2002. SIP: Session Initiation Protocol, [verkkojulkaisu]. Internet Engineering Task Force [viitattu 30.10.2007]. Saatavissa: http://www.ietf.org/rfc/rfc3261.txt.

Rosenberg, J., Schulzrinne, H. 2002. An Offer/Answer Model with the Session Description Protocol (SDP), [verkkojulkaisu]. Internet Engineering Task Force [viitattu 12.11.2007]. Saatavissa: http://www.ietf.org/rfc/rfc3264.txt.

Schulzrinne, H., Casner, S., Frederick, R., Jacobson, V. 2003. RTP: A Transport Protocol for Real-Time Applications [verkkojulkaisu]. Internet Engineering Task Force [viitattu 31.10.2007]. Saatavissa: http://www.rfc-editor.org/rfc/rfc3550.txt.

Wikipedia. 2007. Adobe Flash [verkkojulkaisu]. [viitattu 12.11.2007]. Saatavissa: http://en.wikipedia.org/wiki/Adobe_Flash.

Wikipedia. 2007. Click-To-Call [verkkojulkaisu]. [viitattu 5.11.2007]. Saatavissa: http://en.wikipedia.org/wiki/Click-to-call.

Wikipedia. 2007. Virtual LAN [verkkojulkaisu]. [viitattu 6.11.2007]. Saatavissa: http://en.wikipedia.org/wiki/Virtual_LAN.

Zar, J. 2006. VOIPSA VoIP Security Threat Taxonomy [verkkojulkaisu]. Voice Over IP Security Alliance [viitattu 1.11.2007]. Saatavissa: http://www.voipsa.net/Activities/taxonomy-wiki.php.