IP telephony review

Set of implementations in Czech academic environment

Best Practice Document

Produced by CESNET led working group on Multimedia transmissions and collaborative environment
(CBPD139)

Author: Miroslav Voznak
September 2010

Document No: GN3-NA3-T4-CBPD139
Version / date: September 30, 2010
Original language : EN
Original title: “IP telephony review, Set of implementations in Czech academic environment”
Original version / date: V1.1 of September 30, 2010
Contact: miroslav.voznak@vsb.cz

CESNET bears responsibility for the content of this document. The work has been carried out by a CESNET led working group on Multimedia transmissions and collaborative environment as part of a joint-venture project within the HE sector in Czech Republic.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 23 8875, relating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3)'.

Table of Contents

Executive Summary

In this document, I will describe the most considerable VoIP implementations at Czech universities. In Czech EDU, IP telephony appears with the following features:

- used only in combination with legacy PBX, i.e. no pure solution of IP telephony being used currently,
- Czech universities are involved in the CESNET project of IP telephony and can call each other free of charge (more than 40 VoIP gateways are registered in the CESNET project which started up in 1999),
- IP telephony can be easily implemented as an option for existing PBX and with proprietary protocols (e.g. Siemens, Avaya, Alcatel, …)
- the legacy PBX without possibility of IP telephony is mostly combined with Cisco Call Manager,
- only four universities offer IP telephony based on open-source solutions (based on Asterisk and OpenSER).

At first, I provide an brief overview of scenarios used. The motivation for deploying each scenario derives from user needs but what is the rationale behind implementing VoIP? I see two basic rationales:

- the first being an economic impact,
- the second being an easier integration of information resources into communications.

Czech universities apply three different operation modes:

- PBX's IP trunking: in this mode the existing PBX's of an institution are interconnected through IP (substitution of a simple transmission path with one of very high-level security),
- IP telephony extensions: created accounts can be used in SW or HW IP phones (where open-source solution is implemented, IP telephony is strictly based on SIP),

SIP trunking: as a service offered by providers and including multiple voice sessions, about 70 telecommunications companies provide telephony through SIP in Czech Republic).

1 University of West Bohemia

University of West Bohemia (UWB) is a university located in Pilsen. Its IP telephony is based on the openSER open-source solution and they are using an interesting auto-configuration system (AS). AS enables an automated installation of certain types of Linksys IP phones. It allows multiple phones to be installed without taking up administrators' time usually required to install such phones. The whole Auto-configuration System cooperates with an OpenSER which uses a MySQL database to store its configuration. Once the administrator submits a registration form, the registration systems creates the requested user account in the MySQL database and generates a specific configuration file using a template containing the complete configuration information for an IP phone. The configurations are distributed through TFTP protocol and are downloaded by IP phones when they start up for the first time. Very interesting technical reports were released in the framework of CESNET activity. These reports are by Michal Petrovic from UWB.

- **Security Considerations in IP Telephony Network Configuration**, CESNET technical report 19/2009 [1]. This Technical Report deals with fundamental security settings in networks providing secure VoIP services. Example configurations of Cisco devices are included as well.
- **Manager-Assistant IP Phone Setup**, CESNET technical report 18/2009 [2]. This Technical Report discusses manager-assistant IP phone setup relying on Linksys IP phones.
- **Linksys SPA9xx IP Phone Autoconfiguration System**, CESNET technical report 7/2008 [3]. The Auto-configuration System is designed for an automated installation of certain types of 9xx range IP phones by Linksys. It allows multiple phones to be installed without taking up administrators' time usually required to install such phones.

1.1 Migration to open-source IP telephony

This new solution for IP telephony is based on Linux SIP server with openSER and RTP Proxy. Two identical SIP servers in redundancy mode ensure high availability, one is active and the other one in standby, the redundancy feature is controlled by HSRP protocol. Every server is equipped with two HDD in RAID1, and they are located in separate buildings and designed for 15 000 users.

This solution enables a gradual migration from current Siemens hipath 4000 PBX to openSER. The new IP telephony infrastructure with openSER is built as parallel to legacy PBX. Original university telephony network consists of nine PBX Siemens hipath 4000 interconnected through H.323 with central Gatekeeper Siemens hipath 5000.

The network management supports not only the mentioned migration from Siemens hipath to OpenSER but also IP telephony provisioning that is described in separate chapter.

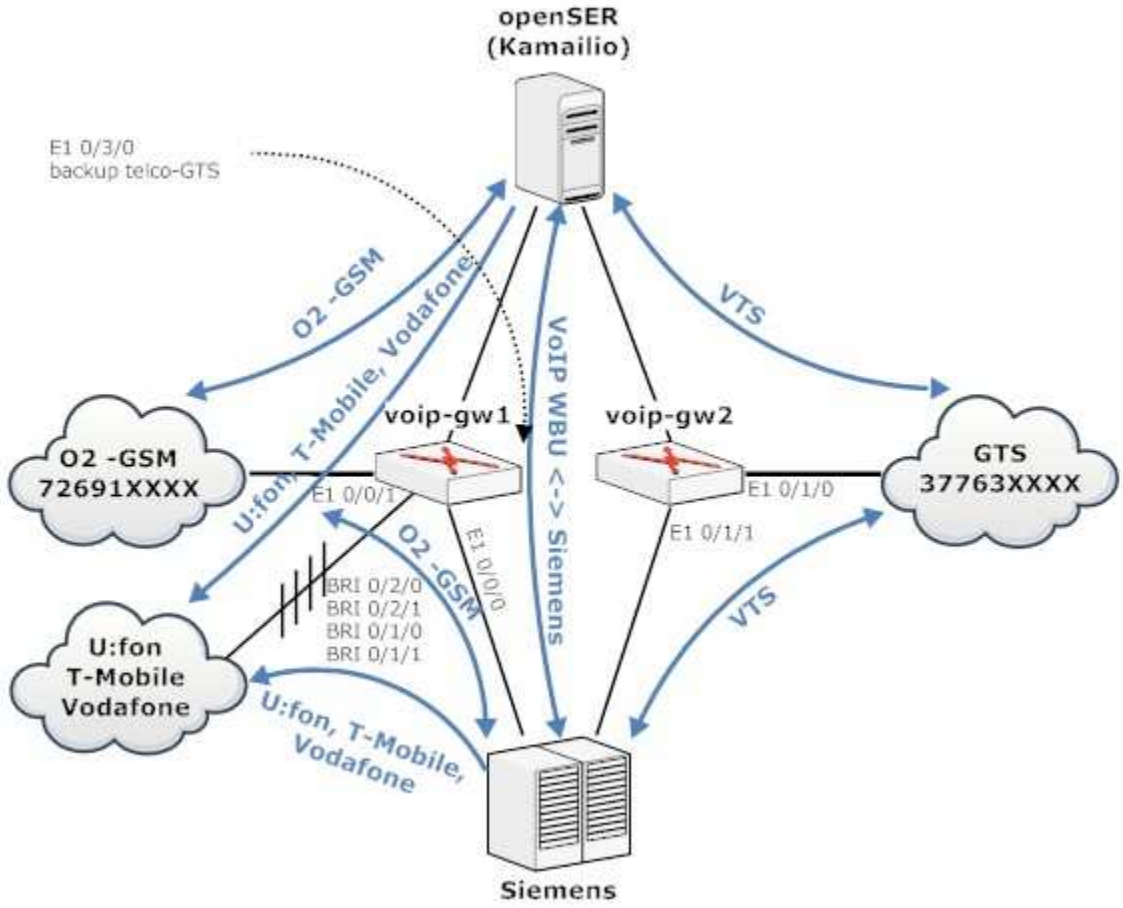

Figure 1: Structure of routing at UWB.

Telco providers are connected to VoIP Gateways (voip-gw1 and voip-gw2) through ISDN, see the figure above, the main DDI is +420 37763 + four digits extensions. Incoming calls are handled by Voice Gateways (Cisco 2851) and forwarded to the appropriate telephone system, either to OpenSER or Siemens hipath. Outgoing traffic is routed through the Voice Gateways to PSTN. Individual gateways are selected based on the least cost routing principle.

1.2 Features of implemented VoIP system

SIP server and Voice gateway are the key elements of the presented solution. OpenSER SIP server is a project spawned from SIP Express Router (SER). It has recently forked into two projects, Kamailio and OpenSIPS. The extent of the features is generally defined by the OpenSER - Kamalio every configuration of openSER is unique and the system can be customized to fulfil any expectation. We briefly summarise the features in this list:

- Compliance with RFC 3261
- Six categories of calls authorization
- Least cost routing

- IP telephony provisioning (Snom, Linksys and Cisco phones are supported)
- Centralized web-based administration of SIP server and Siemens hipath
- User configuration migration from Siemens hipath to openSER
- Multi-address user (more telephone numbers at one SIP account)
- Corporate telephone directory (based on LDAP)
- ENUM
- Forking - parallel ring (one SIP account can be registered at more phones}
- SIP trunks
- Fax
- IP phones behind NAT are supported
- Hunt groups
- Secretary arrangement
- Anti-fraud engine
- SIP server redundancy
- Voice gateway redundancy
- Call forwarding
- Call transfer
- Calling Line Identification Presentation
- Call waiting
- Music on hold
- Do not Disturb
- Third party conference
- Missed calls
- Accepted calls

1.3 Phones provisioning

The provisioning system at this university allows an automated configuration and installation of certain types of 9xx range IP phones by Linksys (SPA921,SPA922,SPA941,SPA942,SPA962). The system consists of several parts:

- Web-based administration interface used to initialize configuration
- LDAP server providing user-specific information used by the Web interface
- DHCP server assigning IP addresses dynamically within pre-defined range
- TFTP server sharing typical configurations to be downloaded by IP phones when they start up for the first time, and also specific configurations for individual phones
- MySQL database storing information on SIP user accounts
- Request Tracker used to track domain name and IP assignments

The Web administration is user-friendly and Linkys phones with firmware versions 5.1.9 and higher offer extended functionality enabling adopt additional information from DHCP server, namely a TFTP server

addresses. In the next step the TFTP server provides a provisional initial configuration referring the IP Phone to a specific configuration.

The System relies on information entered into the Web Interface consisting of a simple form used to register users and generate configuration files to be stored on the TFTP server.

Once the registration form is filled in, the Web Interface also submits a request for an IP address and a domain name to the Request Tracker. Subsequently, appropriate records are created in DHCP and DNS. The IP phone can be connected to the network after the message “registration is successful” was sent to user.

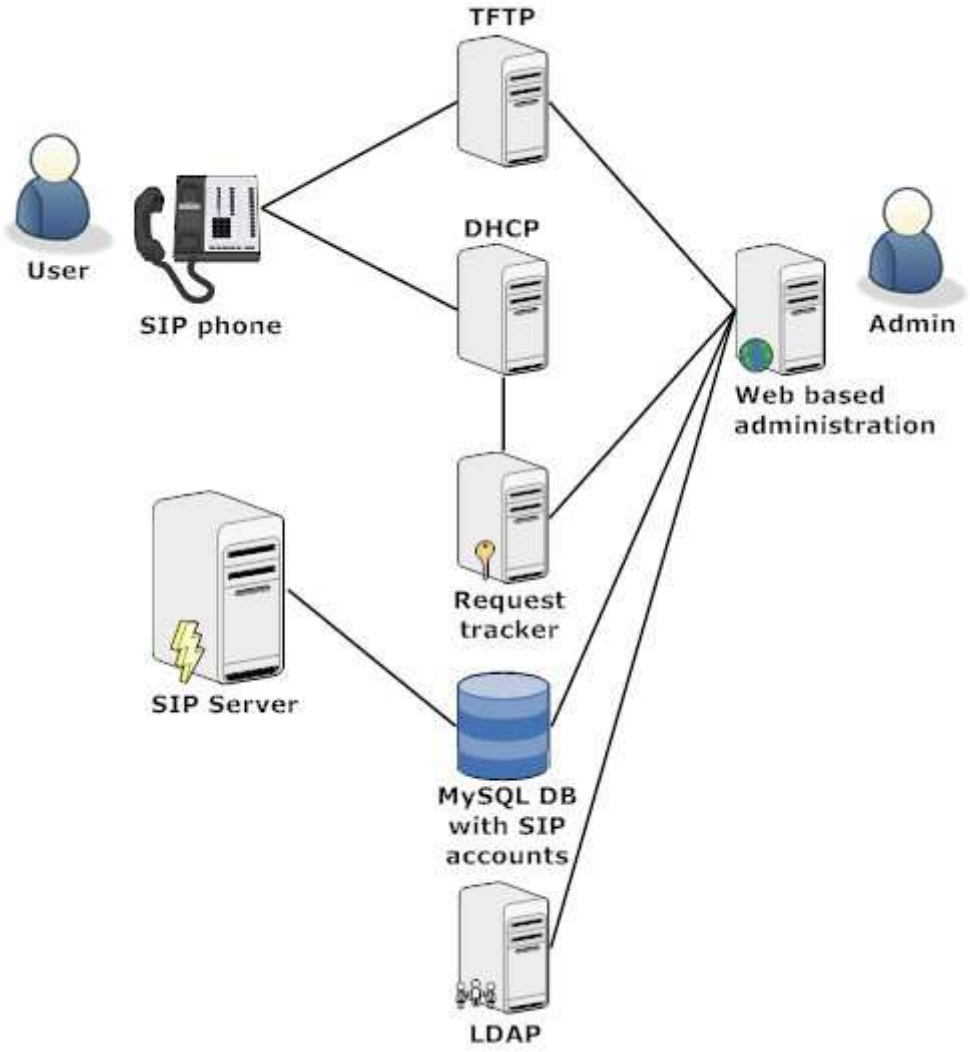

Figure 2: Provisioning system

The key component of the presented provisioning system is the Web administration. Before an IP phone is connected, the administrator has to specify the user's login name. This login is checked against the university information system to get important information for automatic configuration. A simple form follows with most fields pre-filled with information acquired from the LDAP server based on the login name provided earlier. The Administrator actually only needs to fill in the passwords for the user's SIP account. MAC addresses have to be specified for hardware phones, SW IP phones do not require that. Other fields are optional, however it is advisable to fill them in since they provide references to other information systems. These include records such as IP Phone serial number, domain name (hostname), inventory number, or user permission settings.

SIP Passwords are generated automatically since they are only used to configure the IP phones and users do not need to know them. Besides that, the IP phone MAC address and serial number can be now filled in semi-automatically using a bar code scanner. This minimizes the risk of typing errors. All Linksys phones carry appropriate bar codes printed on the outside of their packaging so that it is not even necessary to unwrap them.

1.3.1 Configurations

Every IP Phone must be registered in DHCP and DNS services to obtain IP address automatically. The presented provisioning system relies on DHCP records extended with optional attributes. The number of the relevant attribute is 66 “tftp-server-name” and it contains the IP address of a TFTP server. For example, using the dhcpd.conf configuration file in Linux, the appropriate record looks like this:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
      option tftp-server-name "192.168.1.1";
      ...
  }
```

The TFTP Server needs to be set up to listen to and receive data on UDP port 69. The root TFTP directory contains the initial configuration file used to instruct each IP phone to download its specific configuration. The initial configuration file's name follows the spa<type>.cfg pattern (for example, Linksys SPA922 would require a file named spa922.cfg). IP phones select their specific configurations referring to MAC addresses stored in the $MA format. For example, a specific configuration for a phone whose MAC address is 001122334455 will be found in a file named spa001122334455.cfg, which is referred to in the initial configuration file as /spa$MA.cfg. Other formats may also be used to store MAC addresses. For example, referring the phone to /spa$MAC.cfg will make it look for a file named spa00:11:22:33:44:55.cfg.

The contents of the initial file:

```
<flat-profile>
    <Profile_Rule ua="na">
      tftp://tftpserver.domain/config/spa$MA.cfg
    </Profile_Rule>
    <Resync_Periodic ua="na">
      5
    </Resync_Periodic>
  </flat-profile>
```

The provisioning system cooperates with OpenSER 1.3 using a MySQL database to store its configuration. Once the administrator submits a registration form, the registration systems creates the requested user account in the MySQL database and generates the specific configuration file. User-specific configuration files are generated using a template containing the complete configuration information for an IP phone. The generator simply adds user-related data and stores the resulting XML under the appropriate name. The submitting requests are sent to Request Tracker, DNS and DHCP administrators process such requests and provide DHCP configurations assigning the given IP addresses to phones depending on their MAC addresses. Registration also involves DNS records, which allow the IP addresses to be translated into domain names. When generating requests, newly registered users are given as requesters, which allows them to be notified once the requests for DNS and DHCP registration have been processed.

1.4 Automatic Attendant

An automatic attendant allows callers to be automatically transferred to an extension without the intervention of an operator (typically a receptionist). Department of cybernetics of West Bohemia University applied their own speech recognition algorithms (ASR) to ensure that the called person is recognised and the call transferred to the called party. The automatic attendant at this university is a result of long-term research. The first version was developed in 2003. In addition to ASR technology, the automatic attendant involves using dialogue system based on VoiceXML, Oracle database and text to speech (TTS) technology. The SIP interoperability of automatic attendant is ensured by PJSIP open-source client library, the library is multi-platform and enables to include Asterisk in the overall solution.

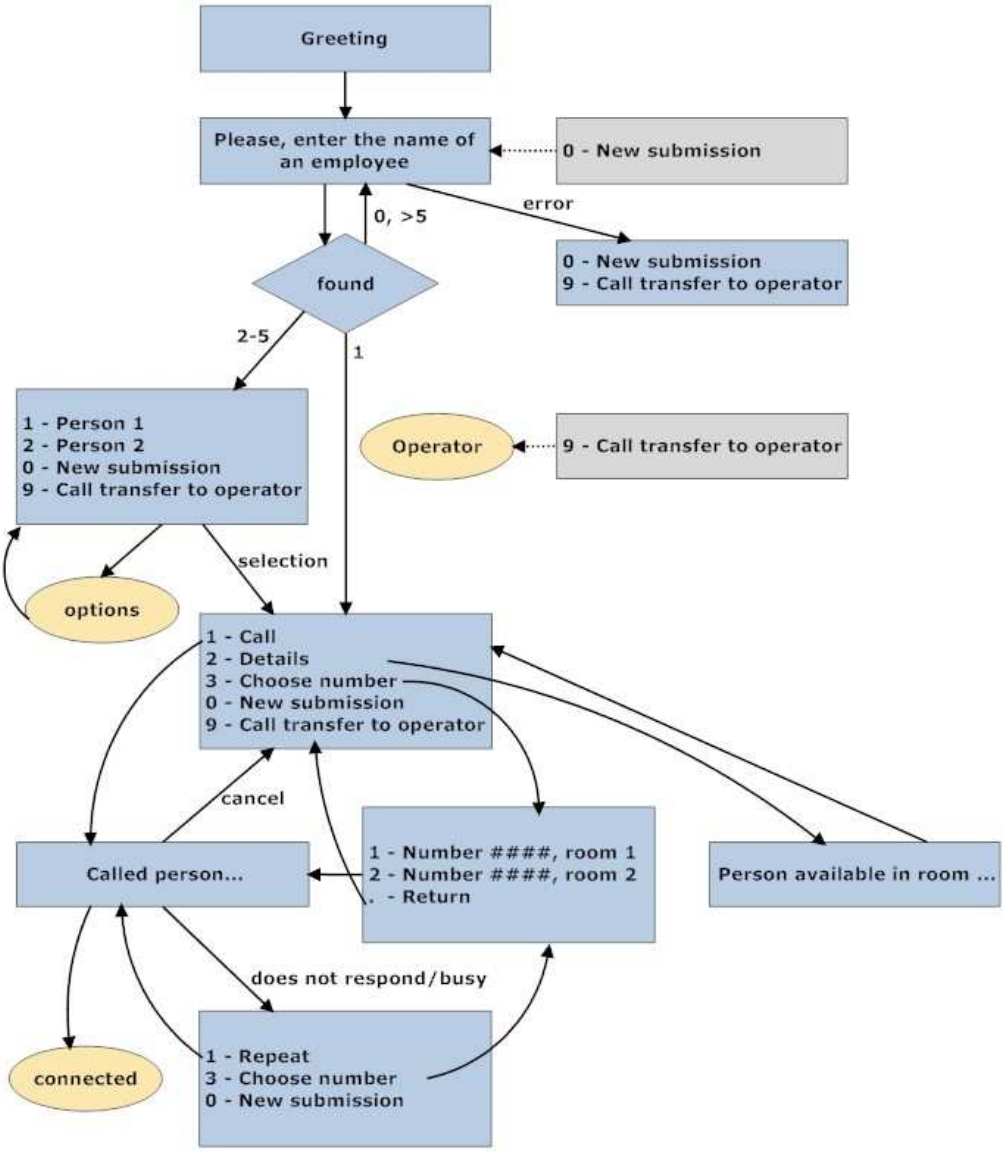

Figure 3: Autoattendant flowchart

Asterisk enables to greet the caller and to replay an announcement. In case the caller is waiting in a call queue, the Asterisk informs him about his position in the queue and finally asks to enter a name of the called person.

The task of auto-attendant is to analyse the speech data, to look the record up in the database and to ensure that the call is transferred to the called party.

Auto-attendant at West Bohemia University was launched in 2008 and nowadays is able to handle four calls simultaneously.

2 Czech Technical University in Prague

Czech Technical University in Prague (CTU) CTU has been using a solution based on Cisco Call Manager (CCM) as an extension of current PBX (Ericsson MD110). Unfortunately, this solution is based on the SCCP proprietary protocol defined by Cisco Systems (originally developed by Selsius Corporation). Besides CCM, this university provides voice services for other CESNET members (more than 20) and this solution is based on H.323. This project began ten years ago and within five years nearly all universities had become involved in it. Every CESNET member owns a PBX which can be equipped with a Voice Gateway (VoGW). This VoGW is registered with Gatekeeper and outbound calls to PSTN are routed through VoGW at CTU. CTU makes out the invoices for voice services. The billing system is fed call detail records (CDR's) from every single gateway through RADIUS protocol, CDR's are stored in Postgree SQL database.

2.1 Infrastructure

In 1999, CESNET launched a project offering voice services based on h323 for universities in the Czech Republic. Every member could connect PBX via Voice gateway to the CESNET network and CESNET provided the key elements including gatekeepers. Two gatekeepers ensured the routing between universities and one gatekeeper offered peering to next NREN's and foreign R&E institutions, calls within this infrastructure were free of charge. The infrastructure was gradually extended by additional gateways and in 2001, it was interconnected to a commercial telecommunications operator. The technical solution of the interconnection to a public telephony network required no investments by CESNET2 (connected through the NIX.CZ exchange point). In the same year, the pilot project for calling into the public network was launched and since January 2002, the access to PSTN has been offered as a service to other members involved in the IP telephony project. Nearly all universities joined in this project and about 40 PBX's connected through gateways were registered in 2005. More than 1.5 million voice calls through the CESNET2 network were carried out, with total duration of 4.5 million minutes a year. It was decided to move the paid voice services (peering to PSTN) to another institution because the CESNET's legal status did not allow for providing the services which are commonly available on the market and many IP telephony providers have arisen at that time. Since 2006, Czech Technical University has been providing the voice services with peering to PSTN.

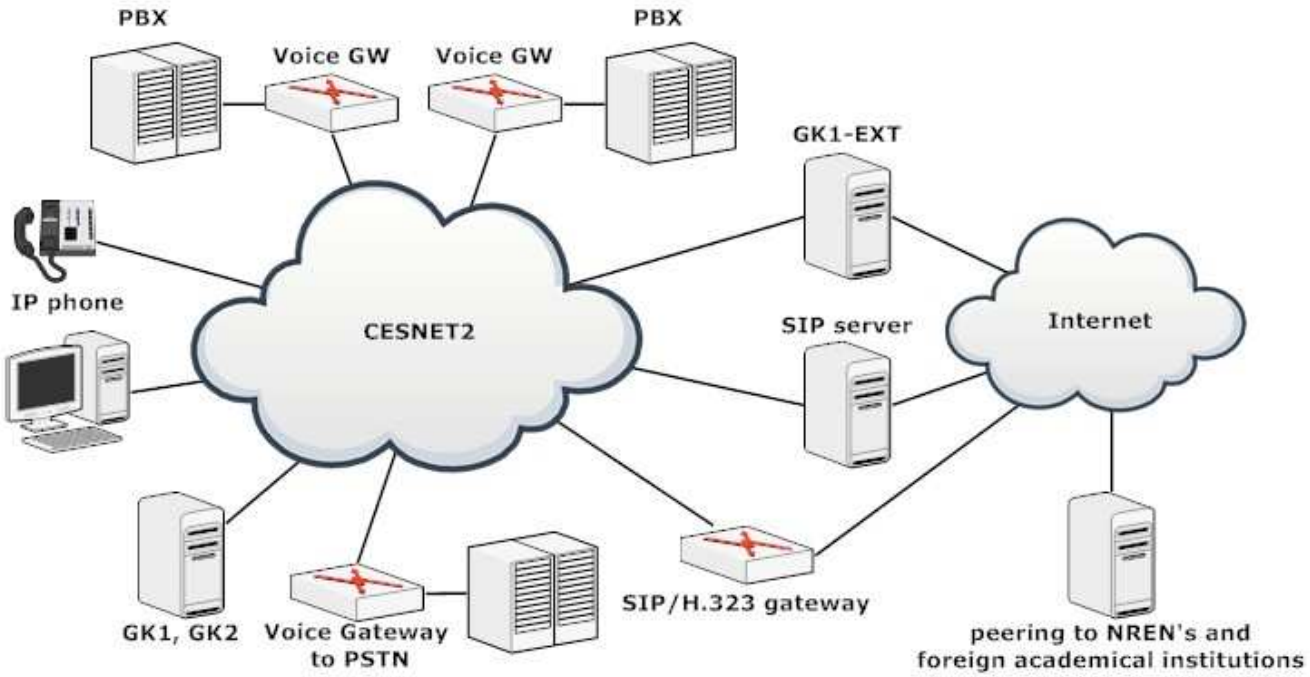

Figure 4: Scheme of telephony network elements used by CTU

The infrastructure is natively based on h323 because its design dates back to 1999. Nowadays, there are gateways without appropriate support - widely used SIP protocol. SIP elements have been fully supported by CESNET during the last five years and cooperation with h323 VoIP infrastructure is realized through SIP/H.323 gateways based on Cisco IP2IP located at CESNET. Certain equipment is able to support both protocols, e.g. Asterisk can serves as SIP/H.323 gateway too.

2.2 Accounting

Provision of paid services needs an application enabling administering tariff tables and accounting for calls made by a particular entity. Czech Technical University operates TAS-IP IP telephony accounting application based on data collected from voice gateways which send information about individual calls through the RADIUS protocol.

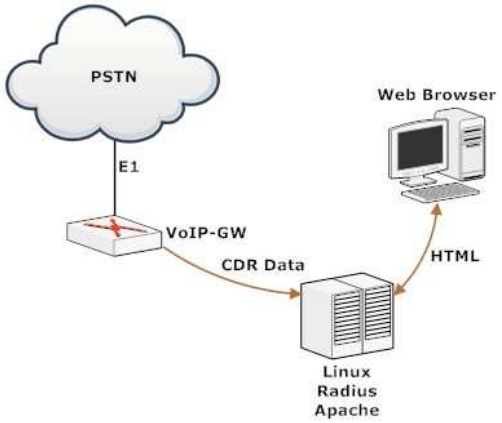

Figure 5: CDR Reports using RADIUS protocol

TAS-IP enables generating both call detail reports and summary reports. Invoices are sent to individual institutions, the calls performed between universities within the CESNET network are free of charge and calls to PSTN are processed by the TAS-IP billing engine which rates and bills.

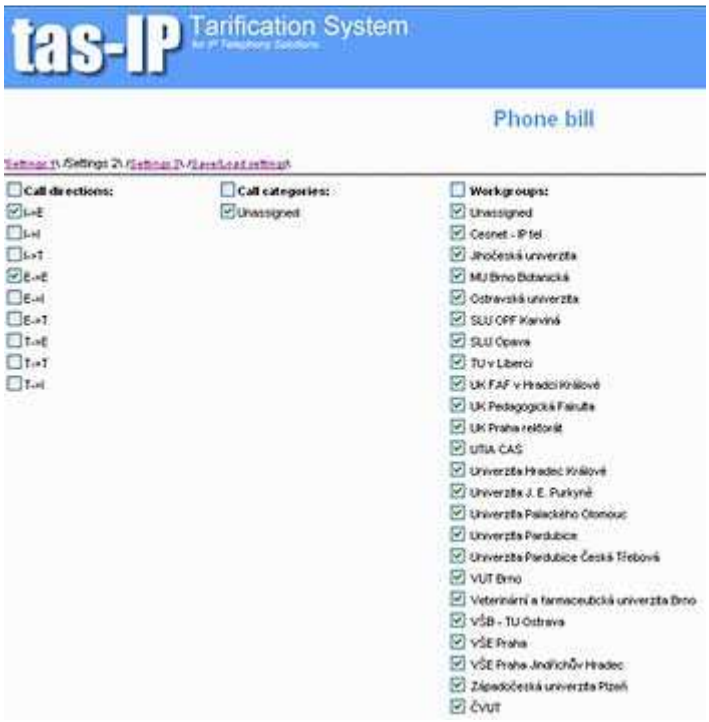

Figure 6: Interface of TaS Billing System

Through RADIUS, CTU collects not only information for billing but also data about the quality of individual calls. Records are imported into an SQL database which serves as the data resource for own evaluation of the web interface. Cisco gateways evaluate sent Icpif value (Calculated Planning Impairment Factor) calculating estimated speech quality. This speech quality monitoring system is described in Technical Report 18/2006 [4].

3 CESNET

CESNET has been focusing on IP telephony for a considerable period of time.. The activity IP telephony in its research plan was established in 1999, in the first period this activity aimed at implementing H.323, later SIP infrastructure have been built up as a parallel to H.323 with translation gateways based on Cisco IP2IP and Asterisk (oh323 channel). Nowadays, advanced services have been implemented. Following technical reports regarding CESNET IP telephony were published in the last couple of years:

- **IP telephony security overview**, CESNET technical report number 35/2006 [5]. The paper provides a basic overview of the IP telephony security and focuses in particular on standardized protocols. Its first part explains mechanisms of authentication in protocols SIP and H.323 and the second part deals with attacks, interdomain trust and DNS.
- **Asterisk and SS7**, CESNET technical report number 26/2006 [6]. Asterisk can interface with both traditional TDM based systems (PSTN networks) and packet based systems (VoIP networks). In our project we focused on interconnecting Asterisk PBX with a PSTN using a Signaling System #7 (SS7) in the role of a call control mechanism.
- **Open Multiprotocol IP Telephony Dynamic Routing System**, CESNET technical report number 20/2006 [7]. The aim of the project is to create a multi-protocol system using SIP, H.323 and MGCP standards, which would ensure routing to various types of VoIP networks. The priority is to provide multi-protocol support to SIP and H.323 signaling and the support of the routing using the ENUM standard (which was to pass from the trial phase into full operation in the Czech Republic in 2007). The document describes the system's architecture and components used. It also briefly describes ENUM. The appendices list supported RFC and describe the configuration of individual components.
- **TLS for SIP Server**, CESNET technical report number 13/2007 [8]. In this report we describe the setup of Transport Layer Security (TLS) in two major open source SIP servers (SER, OpenSer), which are used in the CESNET IP telephony network.

3.1 SIP at CESNET

SIP Proxy is the key element of every SIP infrastructure. SIP Proxy at CESNET is powered by SIP Express Router (SER). SER provides functionality of REGISTRAR and PROXY server. SIP clients can register with REGISTRAR and communicate through PROXY, the routing is based on a dedicated number prefixes which are assigned to individual institutions within CESNET. We did not compose a new numbering plan but we adopted the well-known public telephone numbering plan ITU-T E.164. Almost every phone at any Czech university is available at the same number both within the CESNET network and through PSTN. Where it is not possible to communicate with a particular Voice gateway on SIP, then the call is routed through SIP/H.323

gateway. SIP Proxy also handles entire incoming SIP traffic and certain outgoing traffic to other SIP domains such as iptel.org or bts.sk.

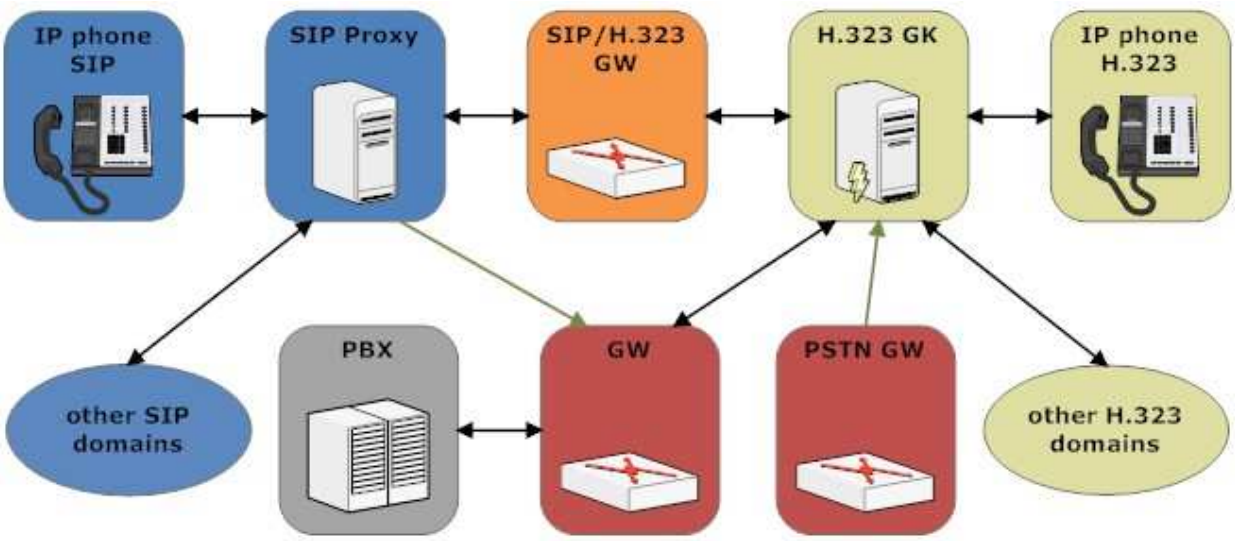

Figure 7: Scheme of telephony elements used by CESNET

The H.323 calls initiated from gateways and from H.323 IP clients are routed through SIP/H.323 gateway based on Cisco IP2IP IOS. CESNET SIP Proxy operates in a multidomain mode. It means that CESNET SER, in addition to its native domain cesnet.cz, is able to handle also other domains of particular universities. Nowadays, CESNET SIP server handles the following domains:

- cesnet.cz
- fel.cvut.cz
- fjfi.cvut.cz
- tul.cz
- uvtuk.cuni.cz
- ics.muni.cz
- czu.cz

The ultimate aim is a direct integration of SIP into communication systems at Czech universities. However, the CESNET multidomain SIP Proxy offers possibilities for trials. Where an institution uses SIP Proxy , DNS SRV record should exist. It can be checked in Linux (host) or in Windows (nslookup).

```
host -t srv _sip._udp.domain
host -t srv _sip._tcp.domain
host -t srv _sips._tcp.domain
```

3.1.1 SerWeb at CESNET

Since 2004, CESNET owns a range of public telephone numbers.The Czech Telecommunication Office assigned an access prefix 950 0 to CESNET, which in the nine-digits national numbering scheme it represents one hundred thousand numbers. These numbers can be used as non-geographical numbers. It means there are suitable for IP phones and for this purpose, an account can be created for any staff at Czech universities.

An account is registered at SerWeb (SIP Express Router Web interface). The new requests are authenticated through the Czech academic identity federation eduID.cz. This federation provides an inter-organizational identity management and access control to network services. The eduID.cz federation is operated by CESNET.

Figure 8: SERweb Interface

The following rules are applied to the calls at CESNET SIP Proxy:

- Only username or telephone number is enough to call within own domain.
- The full SIP URI (username@domain) is necessary for the calls to a foreign domain.
- ENUM is supported too, in this case, the number must be entered in the international format, i.e. 42095001001. The symbol + at beginning of dialled number is not compulsory.

The users registered at CESNET SER are available at SIP URI with username or telephone number and relevant domain. The telephone number is assigned when the account is created.

How to call

A user, who is registered in cesnet.cz domain with username miroslav.voznak and alias 950072003 is available under: miroslav.voznak (within CESNET)

- SIP URI sip:miroslav.voznak@cesnet.cz
- SIP URI sip:950071001@cesnet.cz
- SIP URI sip:420950071001@cesnet.cz
- tel. num. +420950071001 through ENUM
- tel. num. 420950071001 from PSTN (international call)
- tel. num. 950071001 from PSTN (national call)

Testing numbers

- 420950079999
- 420950079999@cesnet.cz
- 420596991192
- 420596991192@cesnet.cz

Free of charge peering

CESNET SIP server provides peering with several VoIP operators in Czech Republic, the calls are free of charge. These operators are listed below:

- VoIPex
- 802.vox
- Fayn
- Ha-vel
- LAM - VaseSit
- NETWAY.CZ
- SITKOM

3.1.2 Institutions available through CESNET SIP PROXY

In addition to access prefix +420 950 0, more then forty PBX's behind Voice gateways are available through CESNET SIP Proxy. The list is provided below:

- Czech Technical University and CESNET, Prague - 224 35x xxx
- Institute of Chemical Technology, Prague - 220 44x xxx
- Czech University of Agriculture in Prague - 224 38x xxx
- University of South Bohemia, Ceske Budejovice - 387 77x xxx, 389 03x xxx
- Charles University in Prague - 224 491 xxx, 224491940, 221 900 xxx, 221 619 xxx, 221 91x xxx, 251 080 xxx
- Charles University, Faculty of Pharmacy in Hradec Kralove - 495 067 xxx
- University of Economics in Prague - 224 092 xxx, 224 094 [1-3]xx, 224 095 xxx, 224 098 xxx, 271 111 xxx, 384 417 [1-3]xx
- University of Pardubice - 466 036 xxx, 466 037 xxx, 466 038 xxx, 465 533 006, 465 534 008
- Technical University of Liberec - 485 35x xxx
- University of Hradec Kralove 493 331 xxx, 493 332 xxx, 493 336 xxx
- Palacky University, Olomouc - 585 63x xxx, 587 32x xxx, 587 44x xxx
- Jan Evangelista Purkyne University in Usti nad Labem - 475 28x xxx
- University of West Bohemia, Plzen - 377 63x xxx
- VŠB- Technical University of Ostrava - 596 99x xxx, 597 32x xxx
- Ostravian University - 597 09[0-5] xxx, 738 51x xxx
- Silesian University, - 553 684 xxx, 596 398 xxx
- The Academy of Sciences of the Czech Republic - 266 05[2-3] xxx, 220 318 xxx, 241 06x xxx, 296 44x xxx, 221 403 xxx, 267 103 [0,1,3]xx,
- The Academy of Sciences of the Czech Republic - 233 087 2xx, 220 390 xxx, 296 780 xxx, 220 390 xxx, 296 780 xxx, 222 828 xxx, 234 612 xxx
- The Academy of Sciences of the Czech Republic - 220 183 [1-5]xx, 286 010 1[1-3]x, 541 517 xxx, 532 290 xxx, 541 514 xxx, 296 792 xxx
- Janacek Academy of Music and Dramatic Arts, Brno - 542 591 xxx, 542 592 xxx

- Masaryk University, Brno - 549 49x xxx
- Mendel University of Agriculture and Forestry, Brno - 545 13x xxx
- Brno University of Technology - 541 14x xxx
- University of Veterinary and Pharmaceutical Sciences, Brno - 541 561 xxx, 541 562 xxx, 541 563 xxx
- Tomas Bata University, Zlin - 576 03x xxx

3.2 ENUM and CESNET

CESNET was very active while ENUM was tested in the Czech Republic. It ensured delegation of appropriate NAPTR records for almost all Czech universities. We recommend to verify the availability of particular numbers.

```
dig -t naptr 8.6.4.0.8.6.4.3.2.0.2.4.e164.arpa
```

Czech ENUM was fully released in 2007, delegation of ENUM 420 prefix was made in 2003 and CZ NIC is the holder of 0.2.4.e164.arpa. CESNET DNS answered the query above and offered both SIP and H.323 service.

```
;; QUESTION SECTION:
;8.6.4.0.8.6.4.3.2.0.2.4.e164.arpa. IN  NAPTR
;; ANSWER SECTION:
8.6.4.0.8.6.4.3.2.0.2.4.e164.arpa. 3600 IN NAPTR 100 50 "u" "E2U+sip"
"!^\\+(.*)$!sip:\\1@cesnet.cz!" .
8.6.4.0.8.6.4.3.2.0.2.4.e164.arpa. 3600 IN NAPTR 200 50 "u" "E2U+h323"
"!^\\+(.*)$!h323:\\1@gk1ext.cesnet.cz!" .
```

In spite of the fact that an ENUM record exists, it does not mean that it is available. In this case, CESNET ENUM monitoring system seems to be useful. Monitoring of ENUM records is based on NAGIOS with check_enum module (plugin) created in PERL. Every prefix is tested using the following procedure:

- existence in WHOIS database
- expiration of validity
- availability of DNS server (NS-SET)
- availability of SRV records in DNS

Service Status Details For Host 'enum.jamu.cz'

Host	Service	Status	Last Check	Duration	Attempt	Status Information
enum.jamu.cz	542591	WARNING	04-09-2009 13:44:13	0d 4h 23m 41s	3/3	Validated for 26 days. It is 1. At least one DNS decsys.vsb.cz. It is 0. 2 of NAPTR records. It is 0
	542592	WARNING	04-09-2009 13:45:49	0d 4h 22m 5s	3/3	Validated for 26 days. It is 1. At least one DNS decsys.vsb.cz. It is 0. 2 of NAPTR records. It is 0

2 Matching Service Entries Displayed

Figure 9: ENUM monitoring interface (JAMU)

If the status returned is WARNING or CRITICAL, the supervisor is informed by email and can subsequently easily find out the reason of fault on the ENUM monitoring web.

Service Status Details For Host Group 'tul.cz'

Host	Service	Status	Last Check	Duration	Attempt	Status Information
enum.tul.cz	48535	CRITICAL	04-09-2009 17:32:08	0d 0h 4m 41s	2/3	Validated for -608 days. It is 2. At least one DNS bubo.vslib.cz. It is 0. 0 of NAPTR records. It is 2

1 Matching Service Entries Displayed

Figure 10: Figure 9: ENUM monitoring interface (TUL)

4 VSB-Technical University of Ostrava

VSB-Technical University of Ostrava (VSB-TUO) VSB-TUO is the third biggest university located in north-east of the Czech Republic. Its IP telephony services are based on two technologies, either on proprietary Hipath technology delivered by Siemens and or on open-source Asterisk. The second one is interesting because its implementation offers many options, e.g. the help-desk of CIT (Centre for Information Technology): the agents of help-desk can log on the call centre based on Asterisk, callers get voice announcement and music on hold while searching for a free agent, if nobody is able to answer the call, another announcement is replayed and the caller can leave a message which is delivered in mp3 format to the helpdesk's email address.

They focus on Spam over Internet Telephony (SPIT) as a real threat for the future. They have developed both a tool generating SPIT attacks and AntiSPIT tool defending communication systems against SPIT attacks. AntiSPIT represents an effective protection based on statistical blacklist and works without participation of the called party which is its significant advantage.

4.1 SPITFILE

SPITFFILE puts much emphasis on the simplicity of using and generating SPIT attacks. SPITFILE was programmed in Python using wxPython GUI and the objective of the designed application is to generate phone calls and to replay a pre-recorded voice message. We adopted the SIPp application which focuses on testing and simulating SIP calls in VoIP infrastructure. SIPp is a open-source test tool or traffic generator for the SIP protocol and can read custom XML scenario files describing from very simple to complex call flows and also send media traffic through RTP. SPITFILE implements a graphic interface for SIPp and works with ready-made .xml diagrams. Thus, the simulation of a SPIT attack is much simpler.

Its control is very intuitive – the requested values are submitted into relevant fields and the SPIT attack is launched by clicking the SEND button. SPITFILE is available both for Linux and for MS Windows. SPITFILE can generate spam in two modes.

- Direct mode, it generates SPIT on IP phone directly without using a SIP Proxy.
- Proxy mode, it generates SPIT via SIP Proxy and thereupon can run against anything that is available behind the Proxy, theoretically involving not only IP phones but also ordinary phones and the whole telephone world. . The proxy mode's menu is depicted below.

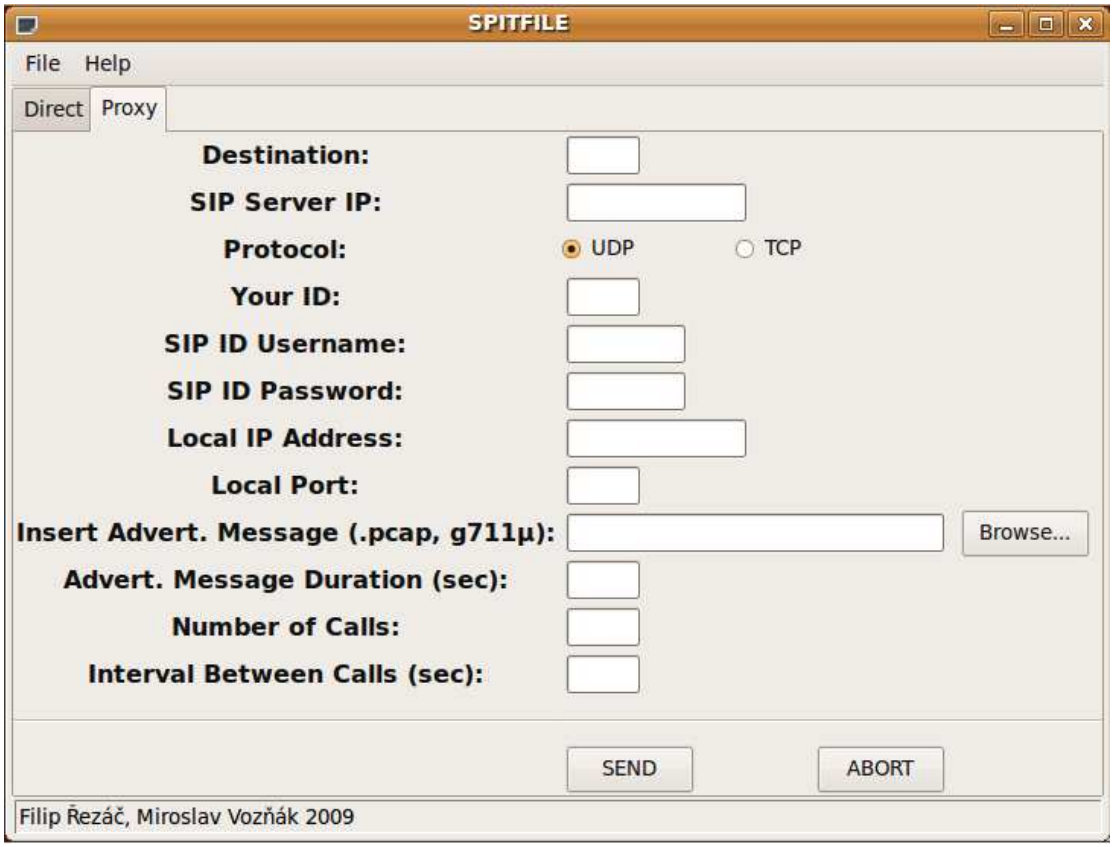

Figure 11: SPITFILE interface in proxy mode

Before SPITFILE can be opened, preconfigured .xml diagrams should be imported into /etc/ directory. Afterwards we can launch SPITFILE and choose one of the two above mentioned attacks that we want to carry out. To run SPITFILE, just type the following command to the terminal:

```
python <location of the SPITFILE.py file>
```

4.2 AntiSPIT

We designed and created our own security application model based on a blacklist which would provide an efficient defence against SPIT. We called the new application AntiSPIT.

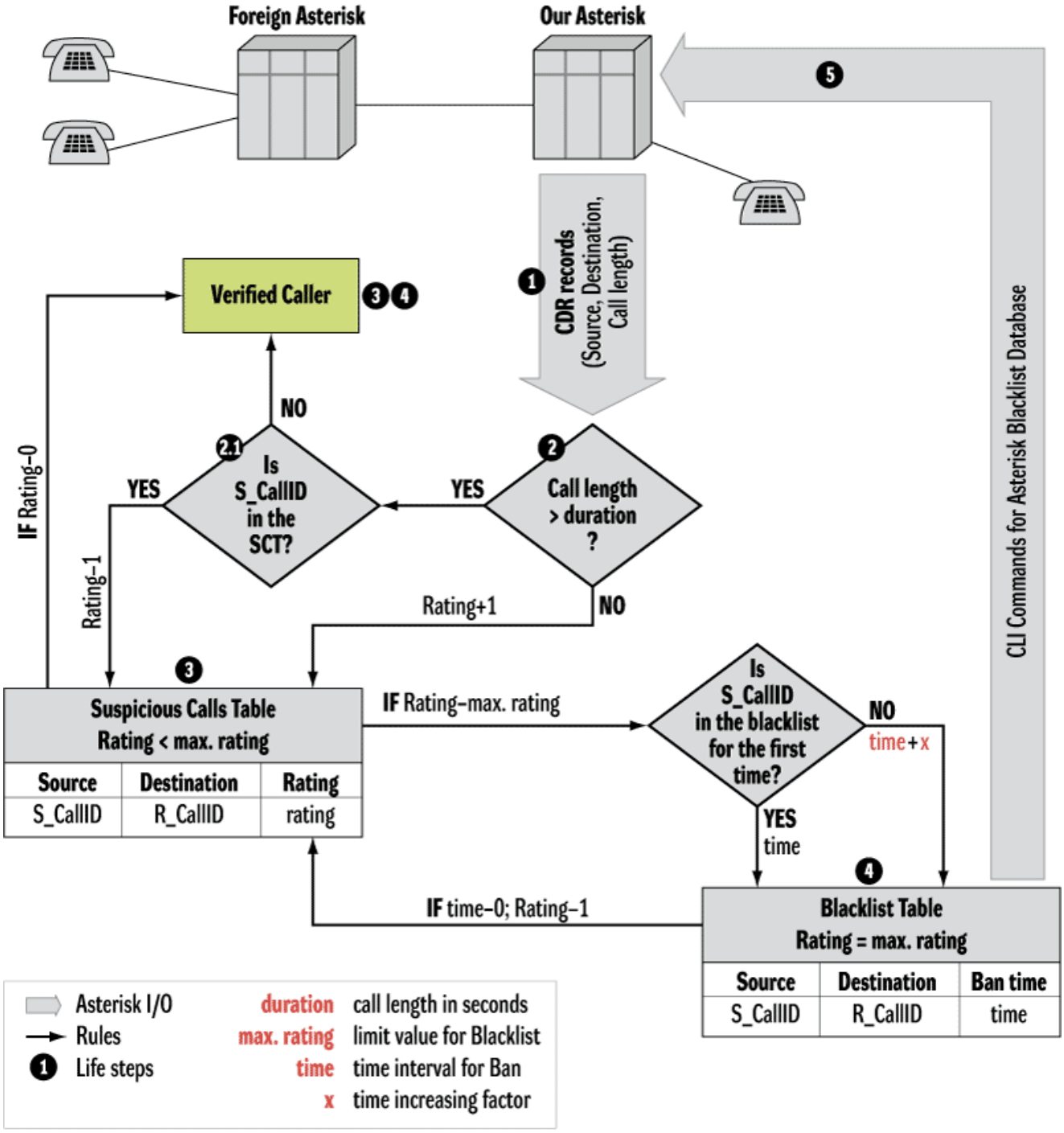

Figure 12: AntiSPIT algorithm

AntiSPIT is able to analyse and process input data from Call Detail Records (CDR's) and consequently determine whether the used source will be inserted into a blacklist. CDR's are an integral part of every PBX and it was decided to implement AntiSPIT also into Asterisk PBX. The application gives an output which is inserted as a command which can control the blacklist. Asterisk provides CLI interface enabling us to create or delete the particular records in the blacklist database. The call duration from CDR's is monitored and if the call duration is less than a certain interval (duration), the source of the calls will receive the status of a suspicious caller and a record with rating is created. In the case of repeated suspicious behaviour the rating will be increased. The maximum achieved rating factor represents a threshold limit value that makes a decision about

whether the record is put into a blacklist table. AntiSPIT has been created in LAMP environment and offers user-friendly administration through a web front-end enabling a user to set the key parameters such as length of call interval (duration), maximum achieved rating factor (max rating), ban time (time). The web front-end also enables monitoring and the management of both SCT table and BLT table.

Figure 13: AntiSPIT web interface menu

The AntiSPIT can be downloaded and freely distributed under the GPL. The CESNET technical report TR 8/2009 [9] deals with security risks in IP telephony, both SPITFILE and ANTISPITE are described in this TR.

5 Ostravian University

Ostravian University (OU) provides IP telephony for their employees with its own developed user-friendly web interface POSERA (PHP OpenSER Administrator). POSERA was implemented in PHP and enables to set up user accounts in OpenSER through the web (HTTPS). The users are verified through LDAP in a corporate directory and then can fill in a form and the new account in OpenSER is created after confirmation. POSERA enables not only creating SIP accounts but also their administration, such as administration of personal information or displaying missed calls.

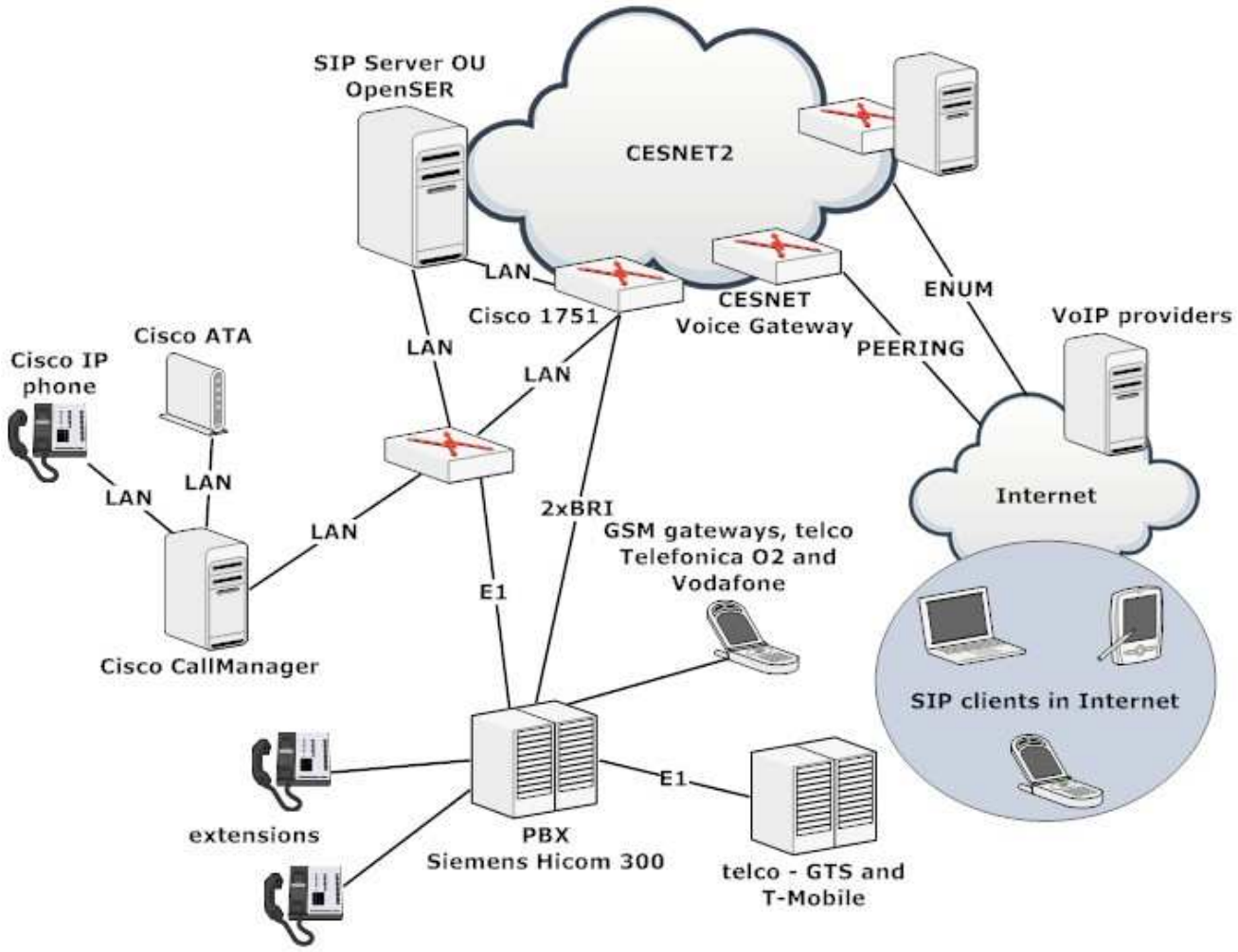

Figure 14: Telephony elements scheme implemented by OU

Topology at OU is not simple, there is a legacy PBX Siemens Hicom300, Cisco Call Manager and OpenSER, Cisco gateways provide the communication between IP and PBX. OU's SIP server was installed in the XEN virtual environment at CentOS. The RTP traffic is routed through the RTP Proxy and it communicates with MySQL DB. OpenSER supports ENUM lookup at OU, the following SRV records are stated in OU's DNS.

```
sip._udp SRV 100 10 5060 sip.osu.cz.
sip._tcp SRV 100 10 5060 sip.osu.cz.
stun._udpSRV 100 10 3478 stun.osu.cz.
```

5.1 OpenSER configuration at OU

The basic OpenSER configuration was created in user-friendly generator SIP wizard. Compared to the default generated in SIP wizard, some changes to the configuration were made. The missed calls are stored in a missed_calls table.

```
# acc_db_request("404", "acc");
acc_db_request("404", "missed_calls");
```

The default 'base-route-invite' configurationdefinining how to handle requests from the Internet enables accepting only requests from pre-defined IP addresses. This behaviour was changed.

```
if(from_gw() || !is_domain_local("$fd"))
{
   $avp(s:caller_uuid) = "0";
   setflag(23);
}
```

The default 'normalize-e164'configuration in SIP wizard is defined to work with a two-digit international prefix. Therefore, a change to accommodate our three-digits prefix 420 had to be made. The used configuration supports the authorization of calls routed to PSTN and the users are authorized in a 'invite-to-external' section route.

```
if(uri =~ "^sip:[0-9]+@")
{
     avp_db_load("$avp(s:caller_uuid)", "*");
     avp_copy("$avp(s:acl_ven)", "$avp(s:caller_acl_ven)/d");
       if (!avp_check("$avp(s:caller_acl_ven)", "eq/ANO"))
       {
          xlog("L_ERR", "PSTN termination unavailable by A
          sl_send_reply("503", "PSTN Termination Forbidden by ACL");
          exit;
       }
   }
```

5.2 POSERA

POSERA is PHP OpenSER Administrator system keeping the same style as the Ostravian University website. Users communicate with the web interface of the SIP server through HTTPS and they are authenticated in LDAP.

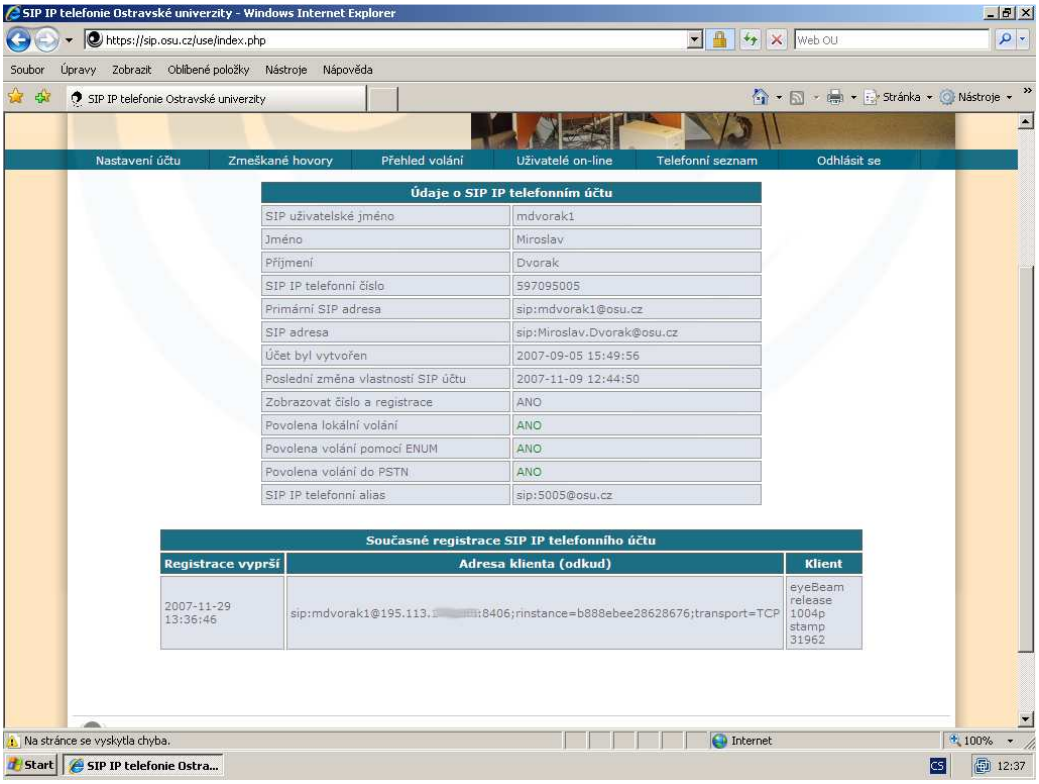

Figure 15: POSERA web interface

6 Interconnecting Asterisk PBX with a PSTN using a SS7

The Asterisk PBX with Signalling System #7 (SS7) support was installed and configured at Cesnet z.s.p.o. The aim of SS7 implementation was to verify a functionality of two SS7 implementations for Asterisk PBX [6]. The tests included interoperability with PSTN switch, signalling procedures verification and load performance tests using SS7 protocol analyzer/simulator [10].

6.1 Signaling System #7

Common Channel Signalling System No. 7 (also referred as SS7, CCS7 or C7) is a suite of control protocols used to provide instructions between elements within a telephony network. SS7 is a digital signalling method that uses a separate (from voice&data network) packet-switched network to transfer messages. That allows reliable and faster connection setup and teardown of a connection and information exchange parallel to the current call. SS7 provides two types of services: (voice-) circuit related and non-circuit related services. First group is used for setup and teardown of voice connections, while non-circuit related services are for example network management or database access for number translations and subscriber information retrieval.

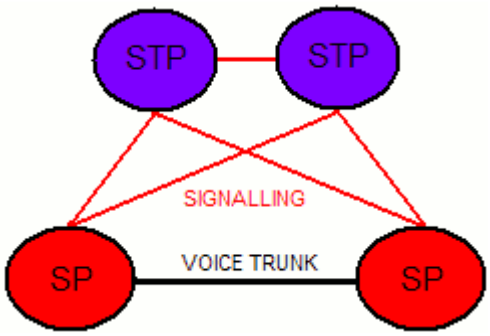

Figure 16: SS7 signalling points

All nodes in SS7 network are called signalling points and they have assigned a unique number the Signalling Point Code (SPC). Nodes in signalling network can be of two types: a Signalling Point (SP) and a Signalling Transfer Point (STP). SP is a source and a destination of signalling messages. STP on the other hand only transfers messages in the signalling network.

6.2 SS7 with Asterisk

Four SS7 solutions can be used with Asterisk: Libisup, ss7box, chan_ss7 and libss7. The two last we had implemented and we performed a lot of tests. Libisup represents a commercial product developed by Cosini Technologies and licensed under the Digium commercial license. The second one, ss7box, was introduced a Digium rival Sangoma and utilizes Sangoma hardware cards. Asterisk SS7 channel driver (chan_ss7) is an open source software developed by Danish company SIFIRA A/S, the license for chan_ss7 is GPL (General Public License) and the solution is not officially certified for the SS7 interoperability. The last one, Libss7, is the latest implementation of SS7 support for Asterisk released by Asterisk developers in summer 2006. Like libisup, it represents a library replacing libpri and making use of chan_zap as channel driver for Asterisk and a zaptel hardware as an interface to SS7 network.

6.2.1 Native Asterisk SS7 support

Libss7 represents the native SS7 support for Asterisk implemented by Digium developers. Libss7 comes in a form of a Linux library replacing the standard ISDN PRI library (libpri). The solution makes use of zaptel channel driver (chan_zap) to control incoming and outgoing calls via the zaptel hardware. It supports only the ITU variant of SS7 implementing MTP2, MTP3 and ISUP protocols. Successful installation of the libss7 library is confirmed by the configure script of asterisk-trunk by finding libss7 and then during process of compilation by creating a chan_zap.so module with libss7 support [6]. Two Asterisk configuration files had to be modified to setup the SS7 connection. The configuration of zaptel device in zaptel.conf is similar as for ISDN PRI. We defined the physical interface parameters (number of E1s, synchronization, framing and coding, etc.), specified the channels used for user traffic and signalling. An example configuration:

```
# span=<span num>,<timing source>,<line build out>,<framing>,<coding>[,yellow]
span=1,0,0,ccs,hdb3
# <device>=<channel list>
bchan=1-15
dchan=16
bchan=17-31
```

The second configuration file zapata.conf is based on a template enclosed with asterisk-trunk branch that can be found in the configs/zapata.conf. We defined the signalling type, SS7 variant, number of linksets, point codes (OPC, DPC) and traffic and signalling channels as shown in the following example.

```
; Signaling type SS7
signalling = ss7
; Variant of SS7 signaling:
; Options are itu and ansi
ss7type = itu
; All settings apply to linkset 1
linkset = 1
; Point code of the linkset
pointcode = 2
; Point code of node adjacent to this signaling link
; (Possibly the STP between you and your destination)
adjpointcode = 1
```

```
; Default point code that you would like to assign to
; outgoing messages (in case of routing through STPs,
; or using A links)
defaultdpc = 1
; What the MTP3 network indicator bits should be set to.
; Choices are national, national_spare, international,
; international_spare
networkindicator=international
; First signaling channel
sigchan = 16
; Begin CIC (Circuit indication codes) count with this number
cicbeginswith = 1
; Channels to associate with CICs on this linkset
channel = 1-15
; another cicbeginwith, so channel 16 is used for signalling
cicbeginswith = 17
channel = 17-31
```

After we configured the zaptel.conf and zapata.conf, we could initialize the zaptel hardware device and load the kernel modules [12].

```
# ztcfg -vvv
# modprobe zaptel
# modprobe wcte11xp
```

After the modules were successfully loaded, we initiated the Asterisk startup. The SS7 link is brought up automatically when Asterisk starts.

Asterisk was successfully interconnected with PSTN at Research and Development Centre for Mobile Applications (RDC) in Prague and tested for call services and related supplementary services against a public PSTN switch - the Ericsson AXE platform.

6.2.2 Asterisk and SS7 Performance Tests

We decide to performe conformance tests according to ITU recommendations Q.784 and Q.785 (with Tektronix K1297) and performance tests (with STT-MSA tester). The tester offered around ten thousands of call requests during a period of about twelve minutes. Call was initiated by ISUP Initial Address Message (IAM) which was acknowledged by Address Complete Message (ACM) sent by remote side. Call answer was signalled by Answer Message (ANM) sent back to initiator. After random period of time the call was released by exchange of Release (REL) and Release Complete (RLC) messages. All behaviour corresponded with ITU recommendations. The graph in Figure 17 displays the total amount of requested calls in testing period (on the left) and the average number of concurrent calls being actively exchanged between PSTN and Asterisk (on the right).

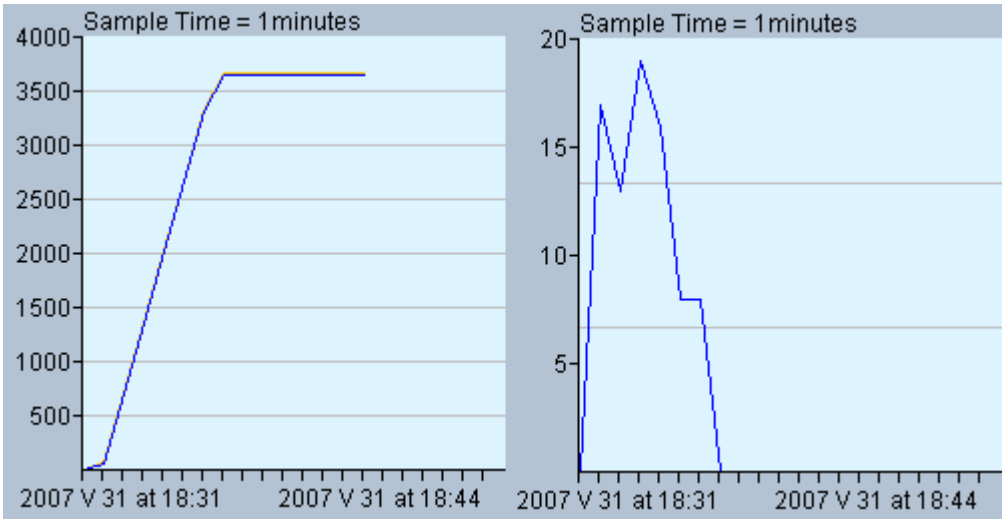

Figure 17: Requested calls in time, average number of served calls, libss7

Initialy we tested the functionality of interconnecting Asterisk PBX server [12] with with public PSTN exchange. We have exchanged calls from PSTN (PLMN) to IVR and to VoIP terminals. In opposite direction calls from VoIP clients via Asterisk were routed to PLMN exchange and terminated on mobile phones. All test calls were successful. SS7 library processed most of MTP and ISUP messages and they proved to be capable of interoperability with PLMN Ericsson AXE exchange. In the next step we performed ITU conformance tests to fully analyze SS7 solutions capabilities. We interconnected Tektronix K1297 protocol tester and Asterisk SS7. We found out that the protocol tester insists on voice channel initialization (group reset) to be done by the remote side. Unfortunatelly none of the SS7 implementations (chan_ss7, libss7) supported the feature. Therefore we couldn't complete the conformance tests. Finally we ran performance tests of Asterisk with SS7 support to test the ability of load processing and unexpected situations handling. STT-MSA protocol analyzer was used to monitor the signalling message exchange. Asterisk with libss7 had problems with serving the offered load. Signalling message exchange differed from the standard, where Asterisk often sent REL message although it is the protocol tester would normally clear the call. And though the release cause in Asterisk messages stated "normal call clearing" more probable cause can be lack of resources for processing the call [10].

7 Kam3cfg, Kamailio configuration script generator

Kamailio configuration script generator (Kam3cfg) represents a tool enabling to configure Kamailio. This tool was developed at CESNET as a generic tool that can be adopted as a suitable solution for Kamailio SIP proxy implementation. Kamailio is very powerful and flexible but its config is difficult to understand. Even more, one small change in the behavior can evoke many changes in the configuration [13].

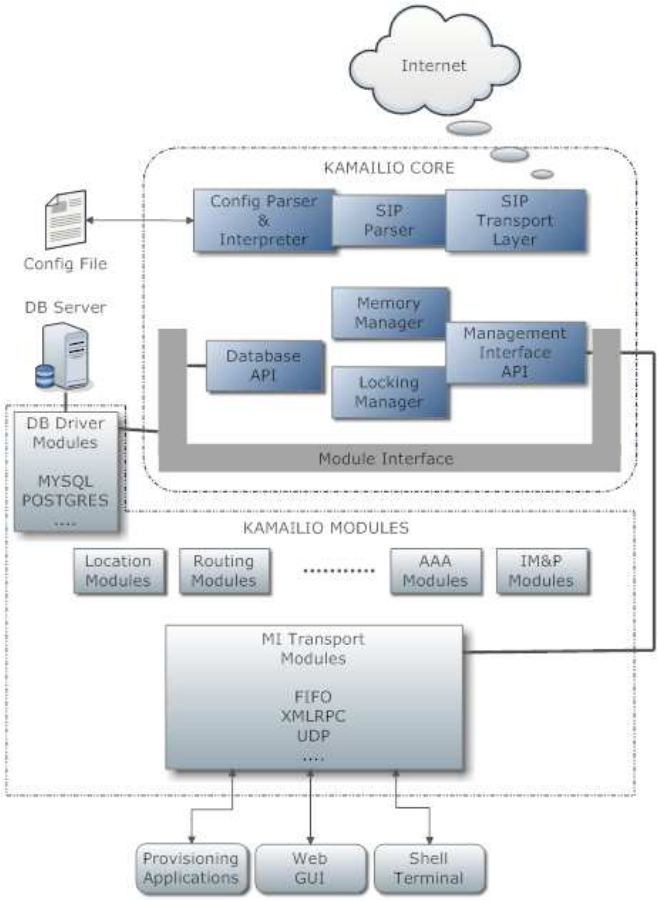

Figure 18: Kamailio architecture

7.1 Kamailio configuration, State of Art

Kamailio has a modular architecture, depicted on figure 18. There are two main components: the core providing the low-level functionalities, and the modules ensuring additional functionalities. The core includes a memory manager, config parser and intepreter, SIP parser, transport layer memory and locking manager, database API and management interface API. The module interface provides access to Kamilio modules. The config file is in fact a script and we need to finetune many parameters to achieve a proper interpretation and interaction with other required technologies such as TLS, MySQL, LDAP or ENUM. The config file consists of many code lines

and many SIP dialogues have to be written directly in it. It is really difficult to create some “generic" config as the code needs to be modifiable by everyone to allow enabling or disabling individual features.

A simple part of a config example is depicted below, a simple modification of one module or feature can cause many changes in the code. For example, in the code, there is a function “is_uri_host_local()” which is a part of one module. This function can be used many times.

```
route[RESTDIALOG] {
 if (loose_route()) {
  if (is_method("BYE")) {
   setflag(1); setflag(3);
  }
  if ($tU =~ +420) {
  } else if ($tU =~ +421 ) {
 t_relay(sip:gw1:5060);
  } else if ($tU =~ +1 ) {
 t_relay(sip:gw2:5060);
  } else if ($tU =~ +47 ) {
 t_relay(sip:gw3:5060);
  }
  route(RELAY);
 exit;
}
```

A Kamailio config file can become a nightmare for many potential users. The new developed tool kam3cfg, which generates the Kamailio config file based on input parameters, is editable so that certain parameters can be modified after its creation. Many users have been waiting for a similar tool and many institutions do not use Kamailio because of the complexity of its configuration file.

7.2 Kam3cfg, script generator

Kam3cfg adopted PHP and Smarty because of their support and portability. Even though there are other powerful languages we wanted to use some templating system and Smarty seemed to be ideal. Many administrators know PHP, it is a well-known language and in combination with Smarty we get a really powerful tool. Smarty is a template engine for PHP. Even though smarty looks like a templating system for HTML pages, it is powerful for other config and text files too. Smarty supports variables, loops, user functions and much more. The configuration below represents the same part of config as in previous subchapter but prepared using Smarty and PHP. Variables are filled in PHP and the rest of work is performed by Smarty. The code is clear and flexible.

```
route[RESTDIALOG] {
 if (loose_route()) {
  if (is_method("BYE")) {
   setflag(1); setflag(3);
  }
<foreach from=$local_prefixes item=prefix>
  if ($tU =~ <$prefix.prefix>) {
  t_relay(<$prefix.gw>);
  } else {
```

```
<foreachelse>
  if (0) {
</foreach>
```

7.2.1 Kam3cfg features

This tool is able to receive arguments also from files and to create config in accordance with requests. The tool has many parameters and explaining all of them is beyond the scope of this document. Only a small number of cases can be seen in examples below. Some parameters can have multiple values. Unfortunately, Console_Getopt module cannot read the same multiple parameters, so we use delimiter ", *" to split it into multiple values. Moreover, all multiple values can be loaded from a file provided it starts with "@". If you want to see all parameters, run "./kam3cfg.php –help".

Example: Simple SBC forcing as RTP proxy.

```
./kam3cfg.php \
  --local-ips 192.168.1.0/24^192.168.3.0/24 \
  --local-domains local.edu^sip.local.edu \
  --local-prefixes '123/556/sip:gw:5060' \
  --force-rtp \
  --listen \
   udp:192.168.1.1:5060^tls:192.168.1.1:5061
```

Example: Simple SBC with NAT traversal.

```
./kam3cfg.php \
  --local-domains @domains.txt \
  --local-prefixes @prefixes.txt \
  --with-nat \
  --listen udp:192.168.1.1:5060
```

Example: Simple SBC with ENUM routing.

```
./kam3cfg.php \
  --local-domains local.edu^sip.local.edu \
  --with-enum \
  --enum-suffixes e164.localnet.edu^e164.arpa. \
  --listen udp:192.168.1.1:5060
```

Xlog suffix and prefix are configurable. Almost any virtual variable of Kamailio can be used. All prefixes will be taken from prefixes.txt and all domains will be read from domains.txt. The file format is one value per line. This is very useful if we have many prefixes and domains. It is important to set local domains, mostly there is only one domain but a multidomain config can be created too. Local prefix, can be served directly by Kamailio or served by an external gateway. The script can use an external LDAP database for authentication, AVP load and local aliases. During each call, a LDAP server is asked to retrieve data.

The big advantage of this script is that it can automatically insert debug messages into the generated script. There are four levels of debug (0-4). A log line can be customized by „xlog-suffix“ and „xlog-prefix“. In a standard kamailio config, this would be more complicated because the log line needs to be changed completely in many places in the script file. More complex scenarios use external databases, such a situation is below where local domains „local.edu“ and „sip.local.edu“ are used. NAT support and LDAP server are enabled. The destination URI is checked against LDAP, therefore an extension should exist in LDAP (achieved by ldapaliases-uri filter).. This option is useful in a multiPBX environment where the central config is at a LDAP server. Even more, LDAP attributes to avps (ldap-attrmap) can be mapped.

Example: More complex example

```
./kam3cfg.php \
  --local-domains local.edu^sip.local.edu \
  --with-nat \
  --with-ldap \
  --with-ldapaliases \
  --ldapauth-uri \'ldap://ldap/o=su?cn,pwd?sub?(|(cn=$au)(number=$fU))' \
  --ldapaliases-uri \'ldap://ldap/o=su?cn,number?sub?(number=$fU)' \
  --ldap-attrmap \'cn=s:username^pwd=s:password^name=s:displayname' \
  --enum-suffixes \e164.localnet.edu^e164.arpa^nrenum.net^e164.org \
  --listen udp:192.168.1.1:5060^tls:192.168.1.1:5061 \
  --with-tls \
  --tls-key '/etc/kamailio/key.pem' \
  --tls-certificate '/etc/kamailio/cert.pem'
```

The tool is available on net [13] and the best way to download it is to follow SVN instructions on the page. Theoretically, with small modifications, this tool could generate configs for Asterisk [13].

References

[1] M. Petrovic, *Security Considerations in IP Telephony Network Configuration*, CESNET: Technical report 19/2009, Prague December 2009.
URL: http://www.cesnet.cz/doc/techzpravy/2009/security-voip-network-config/

[2] M. Petrovic, *Manager-Assistant IP Phone Setup*, CESNET: Technical report 18/2009, Prague December 2009.
URL: http://www.cesnet.cz/doc/techzpravy/2009/manager-assistant-ip-phone-setup/

[3] M. Petrovic, *Linksys SPA9xx IP Phone Autoconfiguration System*, CESNET: Technical report 7/2008, Prague November 2008.
URL: http://www.cesnet.cz/doc/techzpravy/2008/linksys-ip-phone-autoconfiguration/

[4] M. Voznak, M. Neuman, *Monitoring and Measurement of Voice Quality in VoIP Environment*, CESNET: Technical report 18/2006, Prague December 2006.
URL: http://www.cesnet.cz/doc/techzpravy/2006/voice-quality/

[5] M. Voznak, J. Ruzicka, *IP telephony security overview*, CESNET: Technical report 35/2006, Prague December 2006.
URL: http://www.cesnet.cz/doc/techzpravy/2006/voip-security/

[6] J. Rudinsky, M. Voznak, J. Ruzicka, *Asterisk and SS7*, CESNET: Technical report 26/2006, Prague November 2006.
URL: http://www.cesnet.cz/doc/techzpravy/2006/asterisk-ss7/

[7] M. Voznak, J. Ruzicka, L. Macura, *Open Multiprotocol IP Telephony Dynamic Routing System*, CESNET: Technical report 20/2006, Prague December 2006.
URL: http://www.cesnet.cz/doc/techzpravy/2006/voip-routing/

[8] J. Ruzicka, *TLS for SIP Server*, CESNET: Technical report 13/2007, Prague November 2007.
URL: http://www.cesnet.cz/doc/techzpravy/2007/tls-sip-server

[9] M. Voznak, F. Rezac, *Security Risks in IP Telephony*, CESNET: Technical report 8/2009, Prague December 2009.
URL: http://www.cesnet.cz/doc/techzpravy/2009/security-risks-ip-telephony/

[10] J. Rudinsky, *Asterisk and SS7 Performance Tests*, CESNET: Technical report 11/2007, Prague November 2007. URL: http://www.cesnet.cz/doc/techzpravy/2007/asterisk-ss7-performance/

[11] T. Wija, D. Zukal, M. Voznak, *Asterisk a jeho použití*. CESNET: Technical report 12/2005, Praha: CESNET, 2005. URL: http://www.cesnet.cz/doc/techzpravy/2005/voip/asterisk.pdf

[12] J. Van Meggelen, J. Smith and L. Madsen, *Asterisk: The Future of Telephony*. O'Reilly Media, 2005. URL: http://asterisk.stablehosting.net/AsteriskTFOT.zip

[13] L. Macura, M. Voznak, *Kamailio configuration script generator*, In conference proceedings RTT 2010, Velké Losiny, September 8-10,2010, ISBN 978-80-248-2261-7
URL: http://homel.vsb.cz/~voz29/Sbornik_Conference_RTT2010.pdf

[14] L. Macura, *Kam3cfg*, CESNET, 2010, URL: http://open.phonyx.eu/wiki/kam3cfg

Glossary

AS	Auto-configuration System
CCM	Cisco Call Manager
CDR	Call Detail Record
CIC	Circuit Identification Code
DHCP	Dynamic Host Control Protocol
DNS	Domain Name Service
ENUM	E.164 Number Mapping
GPL	GNU General Public License
HTTPS	Hypertext Transfer Protocol Secure
ISDN	Integrated Services Digital Network
ISUP	Integrated Services User-part Protocol
ITU	International Telecommunications Union
LAMP	Linux, Apache, MySQL, PHP
LDAP	Lightweight Directory Access Protocol
MTP	Message Transfer Part of SS7 protocol stack
PBX	Public Exchange
PHP	PHP Hypertext Pre-processor
POSERA	PHP OpenSER Administrator
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
RTP	Realtime Transport Protocol
SER	SIP Express Router
SIP	Session Initiation Protocol
SS7	Signalling System no. 7
TaS	Tariffication System
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TTS	Text to Speech
VoGW	Voice Gateway
XML	Extensible Mark-up Language