Advanced Implementation of IP Telephony at Czech universities

MIROSLAV VOZNAK
Department of Telecommunications
VSB – Technical university University of Ostrava
17. listopadu 15/2172, 708 00 Ostrava
CZECH REPUBLIC
miroslav.voznak@vsb.cz

Abstract: - IP telephony is convenient way of communication and brings number of benefits. One of them is the fact that many services can be implemented in a original way and it opens new field of research and is a challenge for designers of communication solutions especially based on open-source platform. This article describes proposal and advanced implementation of IP telephony which have been arisen in Czech academical environment, concretely in a group of IP telephony acting under Czech Education and Scientific Network association. Author is a senior researcher in this group and he decided to describe the most considerable voice over IP implementations at Czech universities and share knowledge with other experts interesting in IP telephony.

Key-Words: - IP telephony, ENUM, SIP, H.323, Asterisk, OpenSER

1 Introduction

The most considerable VoIP implementations at Czech universities are described in this article. In Czech EDU, IP telephony appears with the following features:

- used only in combination with legacy PBX (Private branch exchange), 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,
- 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 and it is necessary to understand the rationale behind implementing VoIP. I see two basic rationales, the first being an economic impact and the second being an easier integration of information resources into communications. Czech universities apply three different operation modes.

A. 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).

B. IP telephony extensions

The created accounts can be used in SW or HW IP phones (where open-source solution is implemented, IP telephony is strictly based on SIP).

C. SIP trunking

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

The following chapters describe proposal and advanced implementation of IP telephony which have been arisen in Czech academical environment, concretely in a group of IP telephony acting under Czech Education and Scientific Network association (CESNET).

2 Migration from Legacy PBX to Kamailio Project

Kamailio is a continuation of the openSER project. OpenSER was an open source GPL project that aimed to develop a robust and scalable SIP server

and was spawned from SIP Express Router as the well-known free SIP server licensed under the open-source GNU license. The scenario, that is explained in the next subchapters, is implemented at University of West Bohemia (UWB). UWB is a university located in Pilsen in Czech Republic, its IP telephony is based on the Kamailio open-source solution and they are using an interesting auto-configuration system and self-developed automatic attendant with speech recognition algorithms.

Auto-configuration System (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 AS 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 [1].

2.1 Migration to open-source IP telephony

This new solution for IP telephony is based on Linux SIP server with Kamailio (former openSER) and RTP Proxy.

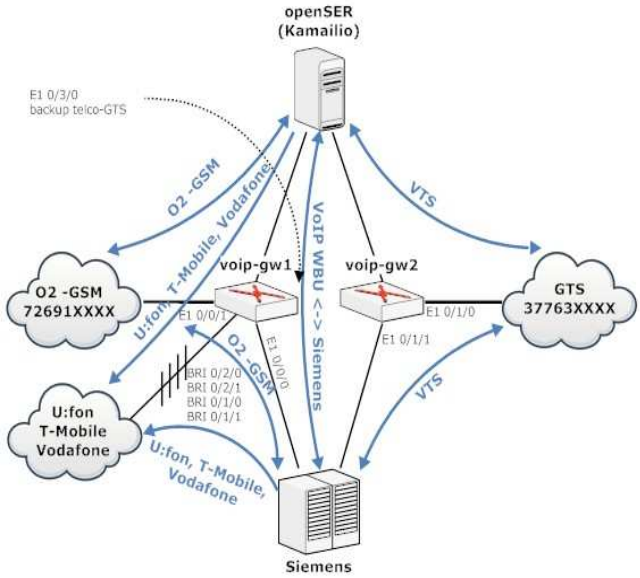

Figure 1. Architecture of the IP telephony at UWB.

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 (Hot Standby Router Protocol). Every server is equipped with two HDD in RAID1 mode, and they are located in separate buildings and designed for 15 000 users. Architecture of the implemented IP telephony at UWB in Pilsen is depicted on Fig. 1.

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.

Telco providers are connected to VoIP Gateways (voip-gw1 and voip-gw2) through ISDN, see the Fig. 1, 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 Kamailio or Siemens hipath 4000. Outgoing traffic is routed through the Voice Gateways to PSTN. Individual gateways are selected based on the least cost routing principle.

2.1.1 Features of implemented VoIP system

SIP server and Voice gateway are the key elements of the presented solution. 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. OpenSER has recently forked into two projects, Kamailio and OpenSIPS, both solutions encompass the same features so far. 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),
- Multi-address user (more telephone numbers at one SIP account),
- Corporate telephone directory (based on LDAP),
- ENUM, mapping E.164 to URI,
- Forking - parallel ring (one SIP account can be registered at more phones),
- SIP trunks,
- Fax, supporting T.38,
- IP phones behind NAT are supported,
- Hunt groups,
- Secretary arrangement,
- Anti-fraud engine,

- SIP server redundancy,
- Voice gateway redundancy,
- Centralized web-based administration of SIP server and Siemens hipath,
- User configuration migration from Siemens hipath to openSER,
- Call forwarding,
- Call transfer,
- Calling Line Identification Presentation,
- Call waiting,
- Music on hold,
- Do not Disturb,
- Third party conference,
- Missed calls,
- Accepted calls,

2.1.2 IP phones provisioning

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

A. Components

The system consists of several parts:

- 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,
- Web-based administration interface used to initialize configuration,
- Request Tracker used to track domain name and IP assignments.

B. Features and characteristics

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 IP phones provisioning system and its interaction with Web based administration is depicted on Fig. 2.

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.

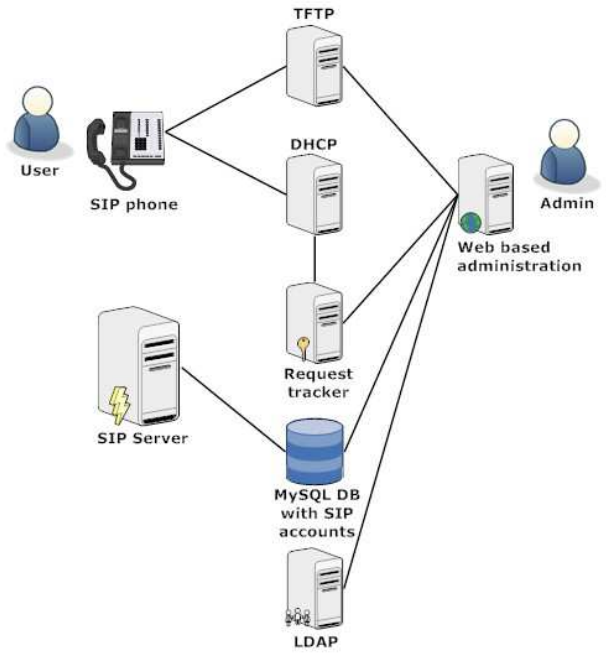

Figure 2. IP phones provisioning system and its interaction with Web based administration.

The key component of the presented provisioning system is the Web administration, see the Fig. 2. 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.

C. 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 [1], [2].

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.

2.2 Automatic Attendant

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. An automatic attendant allows callers to be automatically transferred to an extension without the intervention of an operator (typically a receptionist).

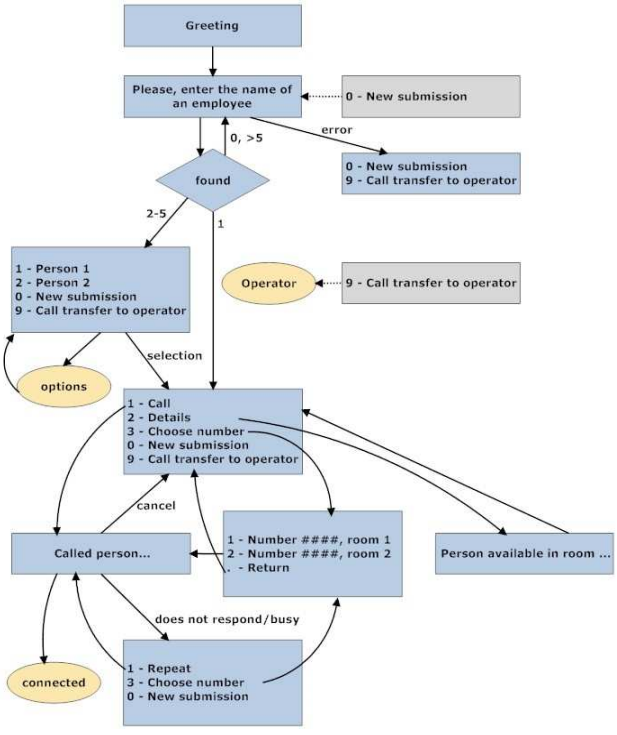

Figure 3. Automatic attendant call flow diagram.

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. The call flow diagram illustrating the request processing in Automatic attendant is depicetd in Fig. 3.

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.

3 Infrastructure Solution

In this chapter, two solutions are described, which provide IP telephony to the other academical institutions and thus have to be adapted to the providing of IP telephony services in EDU infrastructure.

3.1 IP telephony provider in czech EDU

Czech Technical University in Prague (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.

3.1.1 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.

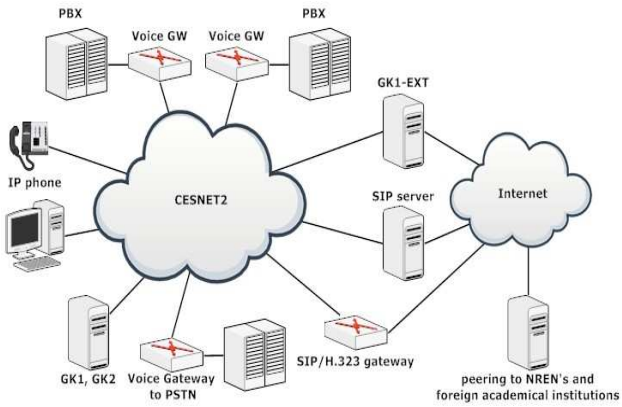

Figure 4. Topology and infrastructure of IP telephony Czech EDU provider.

The infrastructure is natively based on h323 because its original 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 realised 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.

3.1.2 Accounting

Provision of paid services needs an application enabling administering tariff tables and accounting for calls made by a particular entity.

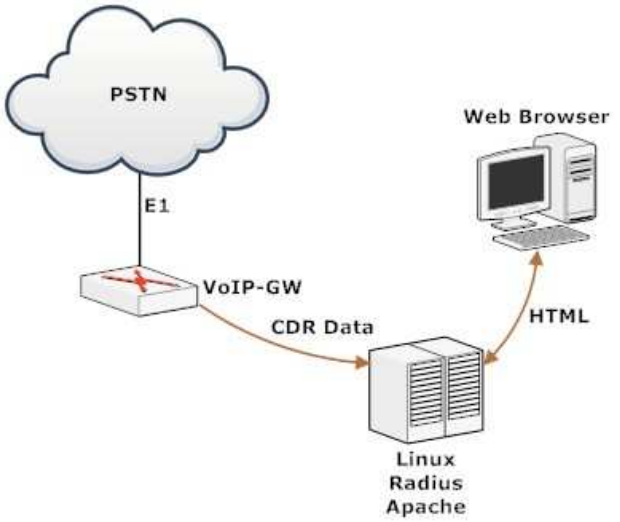

Figure 5. Gathering of Call detail records scheme.

Czech Technical University operates TAS-IP telephony accounting application based on data collected from voice gateways which send information about individual calls through the RADIUS protocol, depicted on Fig. 5.

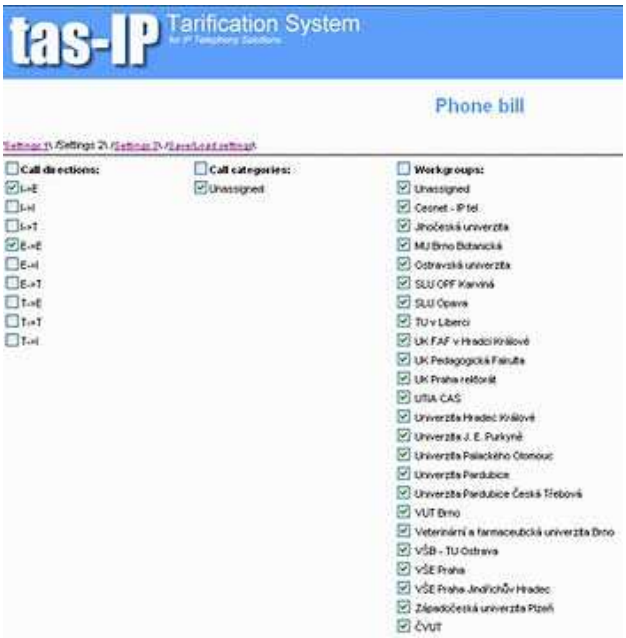

Figure 6. Tarification system, example of screen.

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, an example of TAS-IP screen is depicted on Fig. 6.

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 evaluates sent the Icpif value calculating estimated speech quality (Icpif means Impairment/Calculated Planning Impairment Factor).

3.2 SIP Proxy for all and activities of Czech NREN service provider

The National Research and Education Network (NREN) providers supply the internet services for research and education communities within a country. CESNET (Czech Education and Science Network) is NREN operator in Czech republic and was held in 1996 by all universities of the Czech Republic and the Czech Academy of Science as an association of legal entities [3].

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.

A. IP telephony security overview

IP telephony security overview, CESNET technical report number 35/2006, provides a basic overview of the IP telephony security and focuses in particular on standardised 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 [4], [5].

B. Asterisk and SS7

Asterisk and SS7, CESNET technical report number 26/2006, is focused on SS7 networking. 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 Signalling System #7 (SS7) in the role of a call control mechanism [6], [7].

C. Open Multiprotocol IP Telephony Dynamic Routing System

The aim of the project, described in CESNET technical report number 20/2006, was to create a multi-protocol system using SIP, H.323 and MGCP standards, which had to ensure routing to various types of VoIP networks. The priority was to provide multi-protocol support to SIP and H.323 signalling and the support of the routing using the ENUM standard (which passed 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 the supported RFC and describe the configuration of individual components [8].

D. TLS for SIP Server

TLS for SIP Server, CESNET technical report number 13/2007, describes 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 [9].

3.2.1 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.

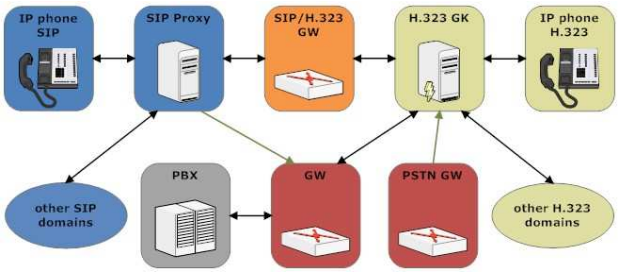

Figure 7. Elements of IP telephony architecture at CESNET.

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. The slements of IP telephony architecture are depicted on Fig. 7. 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
```

3.2.2 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.

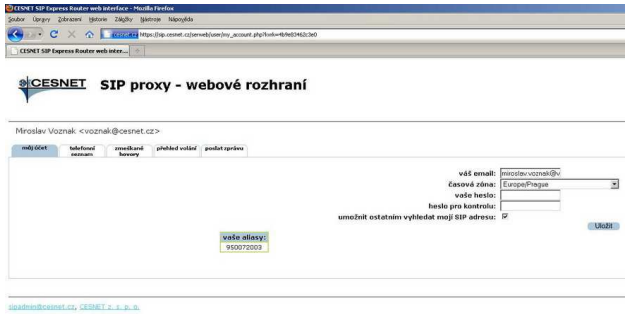

Figure 8. SerWeb screen.

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, Fig. 8, (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.

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.

3.2.3 Call rules within CESNET and peering

An user, who is registered in cesnet.cz domain with username miroslav.voznak and alias 950072003 is available under SIP URI or telephone number

A. Availability and call rules

- 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)

B. Testing numbers

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

C. 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

D. Institutions available through CESNET

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

3.2.4 ENUM in Czech EDU

CESNET was very active while ENUM was tested in the Czech Republic. It ensured delegation of appropriate NAPTR records for almost all Cczech 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 domain. 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, depicted on Fig. 9 and 10), 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

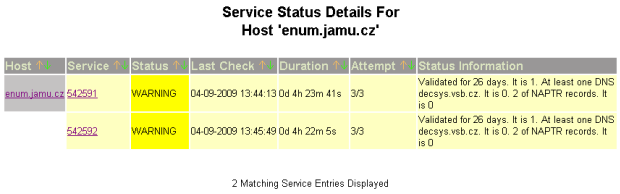

Figure 9. ENUM monitoring, warning status.

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, Fig. 10.

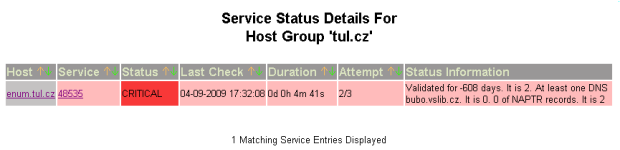

Figure 10. ENUM monitoring, critical status.

4 IP telephony as System Integration

In this chapter, a solution at Ostravian University (OU) is described. This university 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.

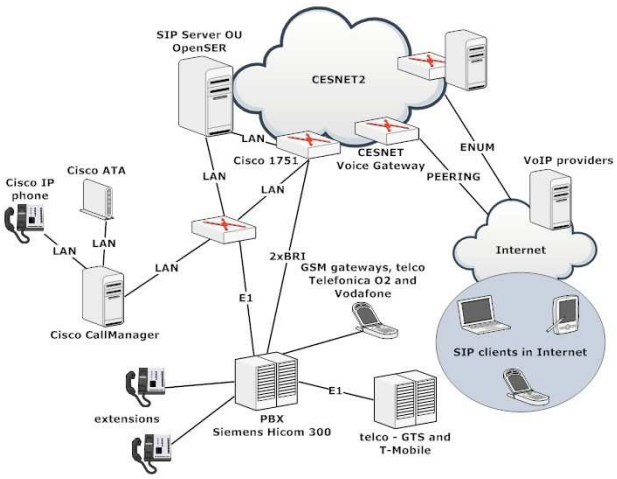

Figure 11. Topology at Ostravian University.

4.1. Topology

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 situation is depicted on Fig. 11.

The RTP traffic is routed through the RTP Proxy and it communicates with MySQL DB [10]. 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._udp     SRV 100 10 3478 stun.osu.cz.
```

4.2 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' configuration definining 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;
    }
  }
```

4.3 POSERA

POSERA is PHP OpenSER Administrator system keeping the same style as the Ostravian University website, depicted on Fig. 12. Users communicate with the web interface of the SIP server through HTTPS and they are authenticated in LDAP.

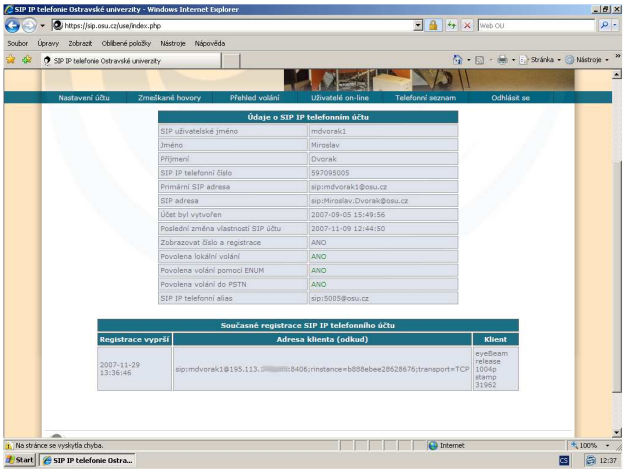

Figure 12. PHP OpenSER Administrator system.

5 Protection against Spam in VoIP

VSB-Technical University of Ostrava (VSB-TUO) is the third biggest university located in north-east corner of the Czech Republic. Its IP telephony services are based on two technologies, either on Hipath technology delivered by Siemens and or on open-source GNU/GPL 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.

5.1. Spam over IP telephony generator

The research activities in the filed of IP telephony were focused on Spam over Internet Telephony (SPIT) as a real threat for the future [11]-[14].

There have been developed both a tool generating SPIT attacks and AntiSPIT tool defending communication systems against SPIT

attacks. The first tool, SPTIFILE, represents a call generator enabling replaying of pre-recorded voice messages, the menu is depicted on Fig. 13.

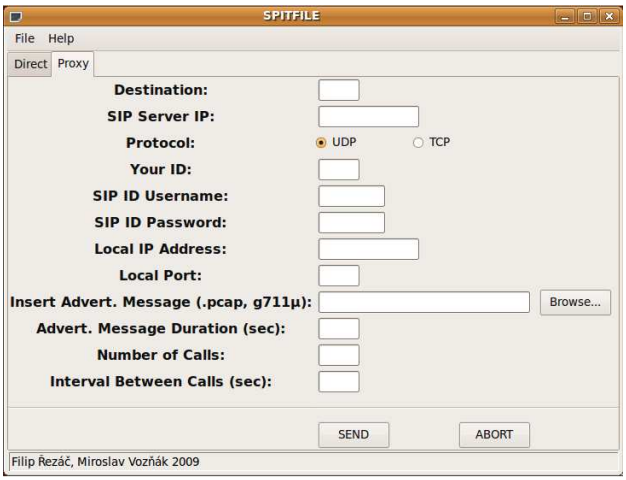

Figure 13. SPITFILE menu.

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>.

AntiSPIT represents an effective protection based on statistical blacklist and works without participation of the called party which is its significant advantage [15].

5.2 AntiSPIT, efficient protection

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, its scheme is depicted on Fig. 14 and described thereinafter.

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.

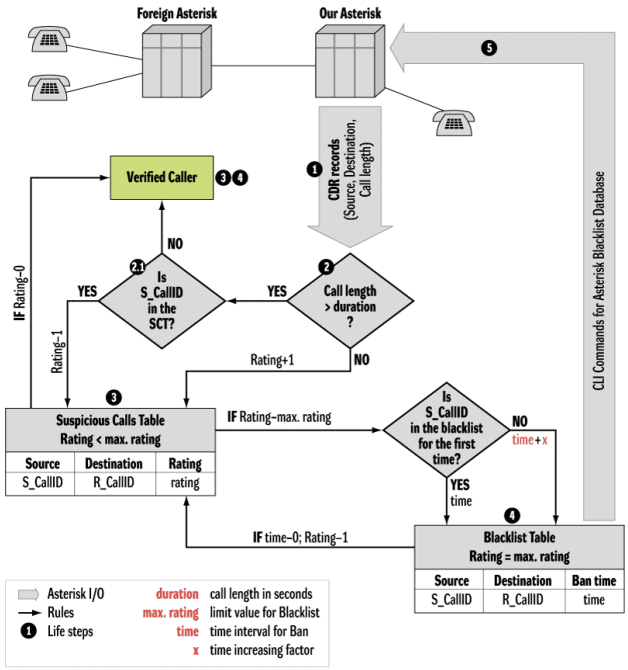

Figure 14. AntiSPIT scheme.

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, Fig. 15.

Figure 15. AntiSPIT Web front-end.

The AntiSPIT can be downloaded and freely distributed under the GPL [16].

6 Approach to Supplementary Services in IP Telephony

This chapter proposes, specifies and describes implementation of DDDS application for supplementary services provision in IP telephony, this method was developed in CESNET IP telephony group in 2009. Supplementary services in traditional telephony were provided by Intelligent Network (IN) concept developed by ITU. One way to implement the services is by convergence with IN and traditional telephony network. Another more recent activity by IETF is represented by direct implementation of the services by protocol SIP. Both solutions are either complex and require changes to be made at client/server side or implement only a relatively small subset of services. An alternative method can be the utilization of existing IP mechanisms. An observation has been made that number of IN supplementary services essentially convert identifiers of calling parties. Therefore ENUM (E164 Numbering Maping), as a mechanism that translates telephony and VoIP identifiers, could be used for the service implementation in IP telephony [17].

6.1 DDDS Application Design

Because ENUM mechanism is limited in the capability to implement maximum number of IN services, new DDDS application is proposed and specified in this text. ENUM mechanism can be described as an application of Dynamic Delegation Discovery System (DDDS). DDDS application represents an abstract algorithm operating on a database with rewrite rules used by the application for string conversion. In order to design an alternative DDDS application to ENUM several parameters need to be defined: Algorithm, Database and Application specific parameters.

6.1.1 Algorithm

General DDDS algorithm was already specified in RFC 3402. The service is provided as a string processing defined by the algorithm, depicted on Fig. 16.

The input is initially converted into a database search key used later to query the database. The key is then matched to database records in order to retrieve rewrite rules for input string conversion. In case a rule is not final, it is applied on the initial input and the search is repeated. Once the terminal rule is reached it is applied on the input string to produce output string for further call processing.

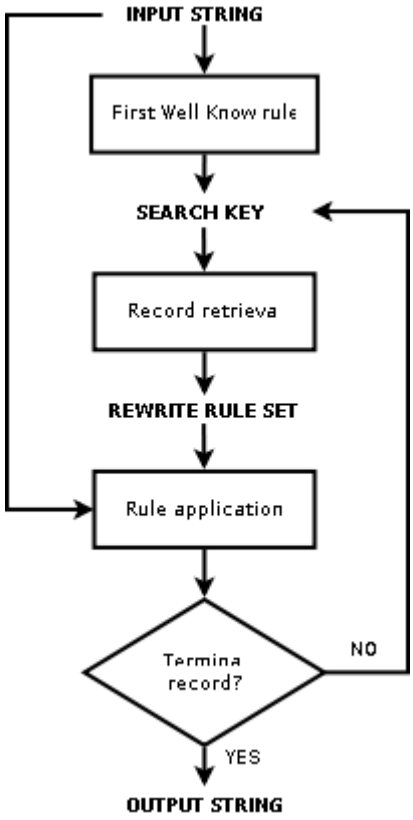

Figure 16. Tarification system, example of screen.

6.1.2 Database

The database contains rewrite rules for string conversion. DDDS specification does not imply any specific database, however a DNS-based hierarchical system has been proposed in RFC 3403. Properties of well known DNS and its scalability make it desirable storage for application rewrite rules. The rules are stored in format of NAPTR resource records.

6.1.3 The Application-Specific Parameters

DDDS application implements the algorithm and makes use of selected database. The application has to specify four parameters:

- Unique input
- First well known rule
- Select database
- Output

A. Unique input

As the application is aimed at identifier translation following input types encoded in UTF-8 are proposed:

- Non-digit string
- Single E.164 number
- Couple of E.164 numbers

An input string must be unique to identify single search path and it has to include complete information to reach desired output. The unique input is used to create a search key and to apply rewrite rule upon to obtain application output. Input can be divided into fixed and dynamic part. Compulsory fixed part is known prior to service execution, while dynamic part changes with every call. Thus the fixed part can be stored in the database as well as used during the search process. Both fractions need to be separated by a delimiter. It should not be any character that appears neither in fixed nor in dynamic input and it should not play primary role in regular expressions (as it is processed by regexp.). Therefore "&" is selected as delimiter. The unique input has been defined by ABNF:

uniq-input = fixed-part delim-char dyn-part
delim-char = "&"
fixed-part = uri / e164number
dyn-part = uri / e164number
uri = <URI as defined in RFC 2396>
e164number = <E.164 phone number>

B. First Well-known Rule

Initial FWKR is applied on the input and provides a database search key. The specification of the rule conforms to rewrite-rules and is represented in the form of regular expression below. FWKR represents an association between the unique input fixed part and the operator domain for service provider identification. When applied the rule provides domain name search key for DNS query:

!^([^&]*)&!\1.OPERATOR_DOMAIN!

C. Select Database

As previously mentioned, proposed DDDS application makes use of DNS to store and query the NAPTR records. The records include regular-expression based rewrite-rule set for string translation. These rules applied to the unique input provide either consecutive search key or final output. The use of the rules represents the service provision in one of three forms:

- Translation of involved party identifier,
- Verification of identifier presence,
- Output selection for routing purpose.

Each rule composes of priority, flags, rewrite rule and service parts. Priority identifies the order in which rules are processed and it can be used for output selection to route the call. Flag indicates, whether a rule is terminal or not and what the following process should be. Rewrite regular expression specifies the translation of string identifier. The regular expression part of NAPTR record for the proposed DDDS application has the ABNF form below. It is composed of two parts. First is regular expression ("ere") that identifies part of the input string intended for subsequent processing. The second part is substitution string ("repl") that contains selected input and an additional part. Application output string is a result of applying the substitution on unique input string.

subst-expr =delim-char ere delim-char repl delim-char *flags
delim-char ="/" / "!" / <char except 'POS-DIGIT' and 'flags'>
ere = <POSIX Extended Regular Expression>
repl = *(string / backref)
string = *(anychar / escapeddelim)
anychar = <any character other than delim-char>
escapeddelim = "\" delim-char
backref = "\" POS-DIGIT
flags = "i"
POS-DIGIT = "1" / "2" / "3" / "4" / "5" / "6" / "7" / "8" / "9"

Finally service field of NAPTR identifies meaning of the record, which has to be unique for every record within a domain (represented by call-party identifier). DDDS application defines two services kinds, where "type" represents a service identifier as specified in ITU recommendation:

- E2E+type = E.164 numbers translation
- E2U+type = E.164 number-to-URI translation

D. Output

Output of the application represents the unique input processed by the rewrite rules. Depending on the service type result can be either E.164 number or URI. However some services require an information whether an input string is present in the database instead. Therefore an error channel is added. DNS provides three response types (below), where the first type is used for return of E.164 number or URI and name error type is used for service check of string presence.

- Record corresponding to queried name and type
- Name error
- Data not found error

6.1.4. DDDS Application Specification

Specification and Description Language, the graphical representation (SDL/GR) is used for formal specification DDDS application and its behavior. The application is realized by a tree

structure composed of "system" as root, "block" as middle layer and "process" as lowest functional element. The system represents application interaction with environment through input and output channels. The blocks model functional elements with simplest interface to each other. The processes define system behavior and are composed of Extended Finite State Machines (EFSM). The system element makes border between the application and the environment. The application is a stand alone process with start up parameters as input channel and a return value as the output. Part of the system are three blocks. Input processing block checks the input parameters such as service type or connection identifiers. Record look up block creates the unique input, applies the first well known rule onto input to produce a search key and finally queries the rewrite rules from the database. Rule application block then applies the acquired rules on unique input to produce output. The output is checked on format and returned by system. Each block contains three processes, whose interaction defines the system behavior.

6.2 Implementation

The application is implemented for functionality verification in IP telephony environment. Out of numerous IP telephony software, Asterisk PBX is selected as a test platform for following reasons.

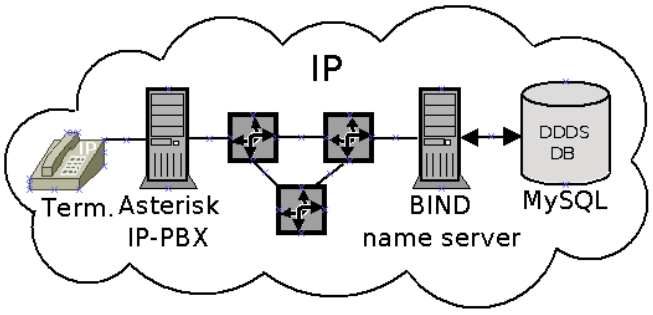

Figure 3. IN-based NP architecture

Asterisk supports SIP, the most common signalling protocol today. PBX is often used by small operators and the possibility to implement IN services can increase their competitiveness on the market. Finally the software has many programmable interfaces that can be used for application implementation. BIND name server is chosen as DNS representative in connection with MySQL database as resource record storage. The architecture is shown on the picture. DDDS application is implemented by shell script (Appendix: DDDS application shell script) and it is portable to other platforms. The script is called by SHELL() function in Asterisk configuration file extensions.conf. The function receives input that contains script path and DDDS application input parameters (such as call party identifiers). It returns the output (identifier), where to connect the call or information about accepting or rejecting the call. Here is an example of Free Phone service:

```
exten => _800XXXXXX,1,NoOp(FPH service called, A=${CALLERID(num)}, B=${EXTEN})
exten => _800XXXXXX,n,Set(Result=${SHELL(/opt/asterisk/bin/ddds_application \
E2E+FPH ${CALLERID(num)} ${EXTEN})})
exten => _800XXXXXX,n,GotoIf($["${Result}" != ""]?default,${Result},1)
exten => _800XXXXXX,n,Macro(incept,1)
```

The format of NAPTR resource record stored by BIND name server and including rewrite rules can have following form:

```
$ORIGIN blue.comtel.cz.
800111112 NAPTR 10 100 "U" "E2E+FPH" "!(^800)(.*)(&.*$)!222\\2!" .
```

DDDS application implementation was verified on Free Phone service. The output from Asterisk follows:

```
-- Executing [800111112@default:1] NoOp("SIP/602336334-084cac8b",
   "FPH service called, A=602336334, B=800111112") in new stack
-- Executing [800111112@default:2] Set("SIP/602336334-084cac8b",
   "Result=222111112") in new stack
-- Executing [800111112@default:3] GotoIf("SIP/602336334-084cac8b",
   "1?default,222111112,1") in new stack
-- Goto (default,222111112,1)
```

The application functionality was verified by implementation in IP telephony system. DDDS application is build as shell script called by Asterisk PBX connected to BIND name server. A Freephone service validatet the functionality of proposed application with positive result [17].

7 Conclusion

This article provides an overview of the significant IP telephony implementations at Czech universities. The advanced best practices are described in individual chapters and all of them are result of research activity in Czech Education and

Scientific Network association. Author is a senior researcher in CESNET and he decided to describe the most considerable voice over IP implementations at Czech universities and share knowledge with other experts interesting in IP telephony.

Acknowledgement
This research has been supported by the "Optical Network of National Research and Its New Applications" (MSM 6383917201) research intent of the Ministry of Education of the Czech Republic.

References:
[1] M. Petrovic, Linksys Autoconfiguration System, *CESNET Technical Report 7/2008*,URL http://www.cesnet.cz/doc/techzpravy/.
[2] M. Petrovic, Security Considerations in IP Telephony Network Configuration, *CESNET technical report 19/2009*, 2009, URL http://www.cesnet.cz/doc/techzpravy/.
[3] M. Voznak, J. Rozhon, SIP Infrastructure Performance Testing, *In Proceedings of the 9th WSEAS International Conference on TELECOMMUNICATIONS and INFORMATICS* , Catania, Italy, May 29-31, 2010, ISBN 978-954-92600-2-1.
[4] F. Rezac, M. Voznak, J. Ruzicka, Security Risks in IP Telephony, *CESNET Conference 2008 Security, Middleware and Virtualization*, September 2008 , Prague, ISBN 978-80-904173-0-4.
[5] M. Voznak, F. Rezac, VoIP SPAM and a Defence against this Type of Threat, *The 14th WSEAS International Conference on COMMUNICATIONS* ,p.172-177, Corfu, July 23-25,2010, ISBN 978-960-474-200-4
[6] J. Rudinsky, M. Voznak, J. Ruzicka, Asterisk and SS7, *CESNET technical report 26/2006*, 2006, URL http://www.cesnet.cz/doc/techzpravy/
[7] J. Rudinsky, Asterisk and SS7 Performance Tests, *CESNET technical report number 11/2007*, 2007, URL http://www.cesnet.cz/doc/techzpravy/
[8] M. Voznak, J. Ruzicka, L. Macura, Open Multiprotocol Dynamic Routing System, *In Networking studies: Selected Technical Reports*, p. 165-178, CESNET, Prague, June 2007.
[9] J. Ruzicka, TLS for SIP Server, *CESNET technical report number 13/2007*, 2007, URL http://www.cesnet.cz/doc/techzpravy/
[10] V. Novotny, D. Komosny, Large- Scale RTCP Feedback Optimization, *Journal of Networks*, 2008, Volume 3, pp. 1-10, ISSN 1796- 2056.
[11] M. Kumar, M. Hemalatha, P. Nagaraj, S. Karthikeyan, A New Way Towards Security in TCP/IP Protocol, *14th WSEAS International Conference on COMPUTERS*, p. 46-50, Corfu Island, Greece, July 23-25, 2010, ISBN 978-960-474-201-1.
[12] J. Asim, U. Shafique, Network Risk Management, *4th International Conference on Communications and InformationTechnology*, p. 141-145, Corfu Island, Greece, July 22-25, 2010, ISBN 978-960-474-207-3.
[13] S. Vincent, J. Raja, A Survey of IP Traceback Mechanisms to overcome Denial-of-Service Attacks, *Proceedings of the 12th International Conference on NETWORKING,VLSI and SIGNAL PROCESSING*, p 93-98, University of Cambridge, UK, February 20-22, 2010, ISBN 978-960-474-162-5.
[14] V. Patriciu, A. Furtuna, Guide for Designing Cyber Security Exercises, *Proceedings of the 8th WSEAS International Conference on INFORMATION SECURITY and PRIVACY*, p. 172-177, Puerto De La Cruz, Tenerife, Canary Islands, Spain, December 14-16, 2009, ISBN 978-960-474-143-4.
[15] A. Sisalem, J. Floroiu, *SIP Security*, JWS, Inc., 350p., 2009, ISBN 978-0-470-51636-2.
[16] M. Voznak, F. Rezac, The implementation of SPAM over Internet telephony and a defence against this attack, *Telecommunications and Signal Processing (TSP) 2009*, Dunakiliti, Hungary, August 2009, ISBN 978-963-06-7716-5.
[17] M. Voznak, J. Rudinsky, Alternative Methods of Intelligent Network Service Implementation in IP Telephony, *The 14th WSEAS International Conference on COMMUNICATIONS* ,p.204-207, Corfu, July 23-25,2010, ISBN 978-960-474-200-4, ISSN 1792-4243

About Author

Miroslav VOZNAK, born in 1971, is an associate professor with the Department of Telecommunications at VSB–Technical University of Ostrava in Czech Republic. He is author or co-author nearly two hunderd publications in information and communications technologies. In this field, he received PhD. in 2002 and habilitation degree in 2009 from Faculty of Electrical Engineering and Computer Science in Ostrava. His research is focused on NGN, speech quality, security and IP telephony. Furthermore, he is a senior researcher in activity "Multimedia transmissions" within CESNET association.