VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

DOHLEDOVÝ SYSTÉM PRO INTERNET PROTOCOL MULTIMEDIA SUBSYSTEM

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

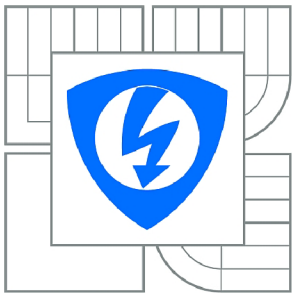
AUTOR PRÁCE
AUTHOR

Bc. MICHAL ŠVEC

BRNO 2013

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

DOHLEDOVÝ SYSTÉM PRO INTERNET PROTOCOL MULTIMEDIA SUBSYSTEM

SURVEILLANCE SYSTEM FOR INTERNET PROTOCOL MULTIMEDIA SUBSYSTEM

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

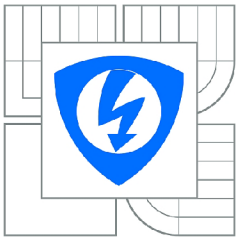
AUTOR PRÁCE — Bc. MICHAL ŠVEC

AUTHOR

VEDOUCÍ PRÁCE — Ing. ĽUBOŠ NAGY

SUPERVISOR

BRNO 2013



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student: Bc. Michal Švec ***ID:*** 110432
Ročník: 2 ***Akademický rok:*** 2012/2013

NÁZEV TÉMATU:

Dohledový systém pro Internet Protocol Multimedia Subsystem

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je prostudovat a popsat subsystém IMS (IP Multimedia Subsystem) z pohledu IMS Core prvků (funkčnosti, možné implementace, signalizace, atd.). V rámci práce se také seznamte s možnostmi shromažďování dat ze školní experimentální IMS sítě (CSCF a HSS prvků). Na základě teoretické studie vytvořte návrh dohledového systému pro školní síť s popisem principu zjišťování dat z této sítě a jejich zpracováním a možností vzdálené konfigurace prostřednictvím navrhovaného systému. Výsledkem práce bude funkční dohledový systém.

DOPORUČENÁ LITERATURA:

[1] POIKSELKA, M., MAYER, G. The IMS: IP Multimedia Concepts and Services. V. Británie: WILEY, 2009. 560 s. Třetí vydání. ISBN 978-0-470-72196-4.
[2] RUSSELL, T. The IP Multimedia Subsystem (IMS): Session Control and Other Network Operations. V. Británie: Mc Graw-Hill OSBOURNE, 2008. 242 s. ISBN 0071488537.

Termín zadání: 11.2.2013 ***Termín odevzdání:*** 29.5.2013

Vedoucí práce: Ing. Ľuboš Nagy
Konzultanti diplomové práce:

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Diplomová práce se zabývá popisem IMS (IP Multimedia Subsystem) subsystému z pohledu IMS core prvků (popis funkčnosti, různé implementace, signalizace atd.) Jsou zde stručně popsány dva hlavní komunikační protokoly SIP a DIAMETER a taky protokol SNMP použitý ke zběru dat pro monitoring systému. Práce popisuje různé IMS projekty spolu s Open IMS projektem, na který byl navržen dohledový systém. V další části se práce věnuje návrhu architektury dohledového systému spolu s možnostmi spravování vytvořeného dohledového systému z pohledu uživatele a administrátora.

Hlavní část diplomové se zabýva popisem dohledového systému pro experimentální školní Open IMS síť a popisuje možnosti vzdálené konfigurace core prvků a monitorování síťového provozu spolu s monitorováním vytížení serverů. V navrhnutém dohledovém systému je většina dat spracována do přehledných grafů, které jsou pravidelně aktualizovány. Závěrečná část se věnuje samotné konfiguraci a implementaci monitorovacích systémů MRTG a NfSen, které byli využity při tvorbě webového dohledového systému.

KLÍČOVÁ SLOVA

IMS, multimédia, služby založené na IP protokolu, multimediální zprávy, SIP, GSM, mobilní síť, VoIP, CSCF, HSS, databáze, DIAMETER, dohledový systém.

ABSTRACT

The master's thesis describes IMS (IP Multimedia Subsystem) in terms of IMS core elements (functional description, different implementation, signaling etc.) Communication protocols SIP and DIAMETER, together with SNMP protocol, which is used for collecting data are briefly described in this thesis.Thesis is also describing various IMS projects together with Open IMS project, for whom was this surveillance system designed. Next part deals with architecture design of surveillance system along with management options implemented in surveillance system for users and administrators.

The main part of master's thesis deals with the description of the surveillance system for the experimental school Open IMS network and describes the remote configuration of core elements and monitoring of network traffic, together with the monitoring servers performance. The most of the data in the designed surveillance system are processed into graphs, which are regularly updated. The final part of master's thesis describes the configuration and implementation of monitoring tools MRTG and NfSen that were used in created web based surveillance system.

KEYWORDS

IMS, multimedia services, IP based services, multimedia messaging, SIP, GSM, mobile network, VoIP, CSCF, HSS, database, DIAMETER, surveillance system.

ŠVEC, Michal *Dohledový systém pro Internet Protocol Multimedia Subsystem*: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2013. 94 s. Vedoucí práce byl Ing. Ľuboš Nagy

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Dohledový systém pro Internet Protocol Multimedia Subsystem“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

Brno ....

(podpis autora)

PODĚKOVÁNÍ

Ďakujem vedúcemu diplomovej práce Ing. Ľubošovi Nagyovi za účinnú metodickú, pedagogickú a odbornú pomoc, za konzultácie a za ďalšie cenné rady pri vypracovávaní tejto diplomovej práce.

Brno ....

(podpis autora)

SIX research centre
sensor, information and communication systems

Faculty of Electrical Engineering
and Communication

Brno University of Technology
Purkynova 118, CZ-61200 Brno, Czechia

http://www.six.feec.vutbr.cz

Výzkum popsaný v této diplomové práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007-13
OP Výzkum a vývoj pro inovace

OBSAH

ZOZNAM OBRÁZKOV

ÚVOD

IP Multimedia Subsystem (IMS) predstavuje súbor špecifikácií, ktoré popisujú architektúru siete budúcej generácie NGN (Next Generation Network), v ktorej sú implementované multimediálne služby.
Prvá kapitola sa zaoberá krátkou históriou a vývojom IMS subsystému. Sú v nej stručne popísané jednotlivé zmeny v IMS subsystéme od predstavenia IMS v Release 5 až po posledný uvedený Release 11 (2012). Ďalej sa kapitola venuje popisu architektúry IMS subsystému. Sú v nej predstavené core prvky IMS (P-CSCF, S-CSCF, I-CSCF a HSS), ktoré tvoria jadro IMS subsystému. V kapitole 1.6 je uvedený popis všetkých rozhraní IMS subsystému. Stručne boli popísané jednotlivé rozhrania medzi prvkami v IMS architektúre vrátane uvedenia komunikačných protokolov, ktoré pracujú na konkrétnych rozhraniach. V prílohe A.1 je uvedená kompletná schéma IMS architektúry z pohľadu rozhraní a entít IMS subsystému.

Druhá kapitola podrobne popisuje dva hlavné komunikačné protokoly SIP a DIAMETER, pracujúce v IMS subsystéme. Kapitola sa venuje predstaveniu SIP signalizačného protokolu, SIP hlavičiek, použitiu SIP metód a taktiež uvádza príklady SIP odpovedí a popis SIP prihlasovania. V kapitole 2.3 je stručne opísaný SNMP protokol, ktorý je určený na výmenu riadiacich informácií medzi zariadeniami pracujúcimi v sieti. V krátkosti sú tu uvedené jednotlivé verzie SNMP protokolu a ich stručná charakteristika.

V tretej kapitole sú predstavené IMS projekty založené na 3GPP špecifikácii IMS/NGN sietí. Najznámejší projekt, Open IMS Core predstavuje implementáciu IMS subsystému, určenú na testovanie IMS aplikácií. Je založený na open source softvéri. Na Open IMS je založená aj školská experimentálna sieť, pre ktorú bude vyvíjaný dohľadový systém. Ďalej je v kapitole 3.6 uvedený projekt NGNLAB. NGNLAB vytvoril webové rozhranie Open IMS Core, určené na lokálnu konfiguráciu potrebných súborov za účelom zmeny IP adries a domény. V tretej kapitole je stručne spomenutý projekt Kamailio, ktorý patrí do skupiny SIP serverov.

Štvrtá kapitola sa venuje definovaniu základných požiadaviek pre IMS dohľadový systém. V kapitole 4.2 je načrtnutá architektúra dohľadového systému z pohľadu komunikácie jednotlivých prvkov Open IMS siete. Sú tu znázornené core prvky Open IMS siete spolu s potrebnými komponentami, ktoré zaisťujú monitoring. Kapitola 4.3 sa venuje návrhu webového rozhrania dohľadového systému a popisuje jednotlivé funkčné prvky. Ďalej sú tu predstavené možnosti prístupu k správe samotného dohľadového systému.

Piata kapitola stručne popisuje jednotlivé zvolené technológie, ktoré boli použité pri tvorbe jednoduchého dohľadového systému pre experimentálnu sieť Open IMS. V krátkosti sú vysvetlené ich vlastnosti a tiež dôvod použitia konkrétnych technológií. Piata kapitola sa zároveň venuje predstaveniu zvolených monitorovacích nástrojov, ktoré boli použité na monitorovanie Open IMS siete.

Posledná časť diplomovej práce sa zaoberá samotnou implementáciu dohľadového systému. Je tu popísaný spôsob komunikácie webového dohľadového systému s core prvkami Open IMS siete a princíp prístupu ku konfiguračným súborom Open IMS siete. V kapitolách 6.3 a 6.4 je popísaná konfigurácia a implementácia monitorovacích nástrojov MRTG (Multi Router Traffic Grapher) a NfSen (Netflow Sensor) použitých pre monitorovanie stavu core prvkov S-CSCF, P-CSCF, I-CSCF a HSS Open IMS siete.

1 IP MULTIMEDIA SUBSYSTEM

1.1 Vývoj IMS

Organizácia 3GPP (3rd Generation Partnership Project), ktorá sa zaoberá vývojom a údržbou GSM, GPRS a EDGE sietí a taktiež štandardizáciou rádiových a chrbticových (*angl. Core Network*) sietí vydala v roku 2000 *Release 2000*, ktorý zahŕňal štandard All-IP, neskôr premenovaný na IMS (IP Multimedia Subsystem). *Release 2000* bol rozdelený na *Release 4* a *Release 5*. *Release 4* bol dokončený bez IMS a obsahoval: MSC (Mobile Switching Centre), MGW (Media Gateway) koncept, IP prenos protokolov pracujúcich na chrbticovej sieti a LCS (Location Services) vylepšenia pre UTRAN (UMTS Terrestrial Radio Access Network).

Relase 5

Relase 5, uvedený v roku 2002, predstavil IMS ako súčasť 3GPP špecifikácií. IMS mal byť štandardizovaný, na prístupe nezávislý štandard, založený na IP architektúre, ktorá spolupracuje s existujúcou hlasovou a dátovou sieťou pre obe pevné (napr. PSTN, ISDN, Internet) i mobilné siete (napr. GSM, CDMA, UMTS). IMS architektúra umožňuje vytvoriť spojenie rovný s rovným (*angl. peer-to-peer*) so všetkými typmi klientov a s potrebnou kvalitou služieb. IMS tiež zahŕňa kompletnú štruktúru služieb (napr. prihlasovanie, bezpečnosť, roaming, platby). IMS tvorí jadro chrbticových IP sietí [4], [36].

Relase 6

Relase 6 bol dokončený v marci, v roku 2007. Predstavil vylepšenia v oblasti smerovania a signalizácie v IMS subsystéme, medzi ktoré patria napr. zdieľanie jednej užívateľskej identity medzi viacerými zariadeniami. Boli štandardizované nové služby, ako sú poslanie multimediálnych správ, konferenčné hovory, PoC (Push to talk over the Cellular service). Ďalšie vylepšenia boli predstavené v oblasti bezpečnosti, spoplatnenia (*angl. charging*) služieb a celkovej architektúry siete [36].

Relase 7

Relase 7 implementoval dve nové prístupové technológie a to DOCSIS (Data Over Cable Service Interface Specification) a xDSL (Digital Subscriber Line). Hlavnými novinkami boli: IMS multimediálne hovory, zaistenie neprerušovaného hovoru (*angl. Voice Call Continuity*), lokálne číslovanie, SMS (Short Message Service) v IP sieti,

pridanie IBCF (Interconnection Border Control Function), vytvorenie relácie pomocou ktorej bude uskutočnené tiesňové volanie, nový autentifikačný model pre pevné siete a ďalšie [36].

Relase 8

V release 8 bola pridaná podpora LTE (Long Term Evolution) a SAE (System Architecture Evolution) sietí. Vylepšené boli možnosti v oblasti centralizácie IMS služieb, zaistenia neprerušovaného spojenia a v oblasti tiesňových volaní (*angl. emergency sessions*).

Relase 9

Release 9 priniesol podporu tiesňových volaní (*angl. emergency calls*) v GPRS (General Packet Radio Service) a LTE sieťach. Dosiahlo sa lepšie zabezpečenie na aplikačnej vrstve IMS subsystému. Bolo taktiež doplnených niekoľko nových možností v oblasti centralizácie služieb a kontinuity (neprerušené spojenie). Zdokonalenia sa dočkali aj multimediálne hovory (VoIP).

Relase 10

Release 10 pridáva možnosť užívateľom ovládať reláciu, v ktorej sú prostriedky poskytované jedným, alebo viacerými účastníckymi zariadeniami (*angl. user equipment*). Ďalší prínos realase 10 bol vo vylepšení tiesňových hovorov, a v SRVCC (Single Radio Voice Call Continuity) neprerušovaných hovoroch.

Relase 11

Posledný uvedený release 11 (2012) implementuje podporu protokolu USSD (Unstructured Supplementary Service Data), ktorý poskytuje spojenie medzi UE a operátorom pomocou krátkych správ, dlhých max. 182 alfanumerických znakov (informácie o polohe užívateľa, informácie o počasí, atď.). USSD je narozdiel od SMS relačne orientovaná služba. Release 11 prináša taktiež možnosť odoslania a prijatia SMS bez MSISDN (Mobile Subscriber International ISDN Number) čísla [2], [3].

1.2 Internet Protocol Multimedia Subsystem

IMS je globálny, nezávislý na prístupe a štandarde IP pripojenia a architektúre, ktorá poskytuje rôzne typy multimediálnych služieb koncovým užívateľom pomocou základných internetových protokolov [36].

Globálny: Z užívateľského hľadiska je dôležité mať prístup k službám nezávisle na geografickej polohe užívateľa IMS subsystému. Roaming umožňuje použiť služby, ktoré nie sú fyzicky dostupné v domovskej sieti.

Vzájomne spolupracujúci: IMS systém nebol nasadzovaný rovnomerne po celom svete, preto je potrebné, aby IMS systém spájal čo najviac užívateľov ako je možné. Preto IMS systém podporuje komunikáciu s ISDN, PSTN, mobilnými i internetovými užívateľmi.

Nezávislý prístup: IMS bol pôvodne navrhnutý tak, aby bol nezávislý na použitom prístupe teda, aby boli IMS služby dostupné z akejkoľvek IP siete (napr. GPRS, WLAN, širokopásmové pripojenie, UMTS atď.). S príchodom Release 5 (GSM) však boli do štandardu pridané niektoré GPRS špecifické funkcie. V Release 6 tieto funkcie týkajúce sa prístupu do GPRS boli odstránené a IMS architektúra bola obnovená na pôvodnú verziu, ktorá bola nezávislá na prístupe [36].

1.3 IMS Architektúra

Tak ako názov IP Multimediálny Subsystém naznačuje, je dôležité, aby zariadenie malo IP konektivitu. Peer-to-peer aplikácie vyžadujú end-to-end dostupnosť, ktorá je najjednoduchšie dosiahnuteľná pomocou IPv6 (IP version 6) adries, ktoré majú dostatok adresného priestoru. 3GPP preto stanovilo, že IMS subsystém podporuje výhradne IPv6 [1]. Avšak počiatočná implementácia IMS a jej nasadenie mohli používať IPv4 (IP version 4) adresy. Prístup k IP sieti môže byť cez domácu sieť (*angl. home network*), alebo cez hosťovskú sieť (*angl. visited network*) [36].

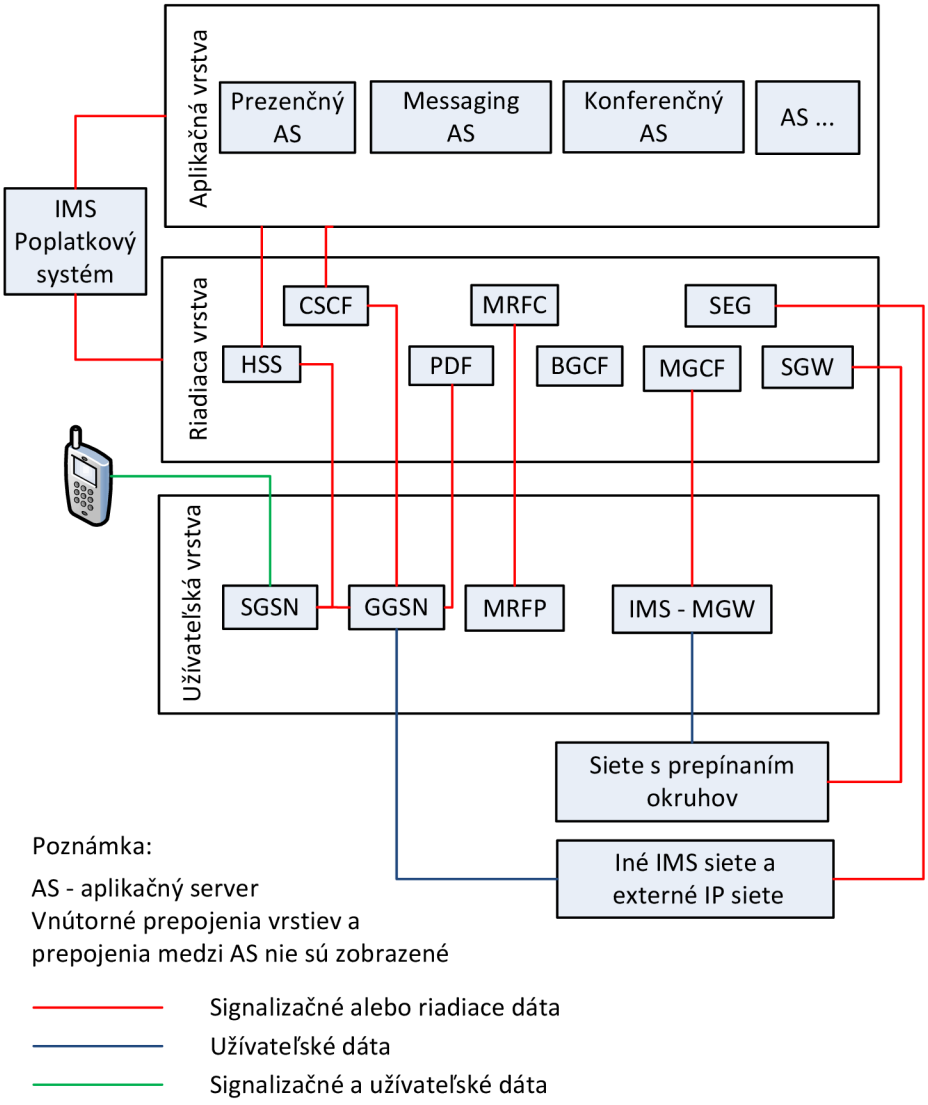
1.3.1 Bezpečnosť komunikácie

Bezpečnosť je základnou požiadavku každého komunikačného systému. IMS má samostatný autentizačný a autorizačný mechanizmus medzi UE (User Equipment) a IMS sieťou z dôvodu prístupu k sieťovým službám (napr. GPRS sieť). Naviac, integrita a voliteľná bezpečnosť SIP (Session Initiation Protocol) správ je zabezpečená medzi UE a IMS sieťou a medzi prvkami IMS siete. Zabezpečenie poskytuje minimálne rovnakú úroveň bezpečnosti ako v GPRS a okruhovo-prepínaných sieťach (*angl. circuit-switched networks*). Napríklad: IMS zabezpečí, aby boli užívatelia autentizovaní predtým, ako môžu používať konkrétne služby. Užívatelia majú možnosť požiadať o zaistenie bezpečnej komunikácie pri spustení relácie (*angl. session*) [36].

1.3.2 Vrstvový model

3GPP sa rozhodlo použiť vrstvový model pre návrh IMS infraštruktúry. To znamená, že transportná vrstva a nosné služby (*angl. bearer services*) sú oddelené od IMS signalizačnej vrstvy a taktiež od riadiacej vrstvy (*angl. management services*). Ostatné služby pracujú na IMS signalizačnej vrstve. Na obrázku 1.1 je zobrazená architektúra IMS subsystému rozdelená do jednotlivých vrstiev. Hlavným cieľom tejto architektúry je minimálna závislosť medzi jednotlivými vrstvami. WLAN (Wireless Application Protocol) prístupová sieť bola implementovaná do IMS subsystému v 3GPP *Release 6* a pevné širokopásmové pripojenie bolo do IMS implementované v *Release 7*. Nezáleží na tom, či užívateľ používa na komunikáciu mobilný telefón alebo počítač, vždy bude použitá určitá skupina funkcií v IMS. [36]

Viacnásobný prístup (*angl. multi-access*), ktorý je implementovaný v IMS architektúre umožňuje nezávislý prístup pre účastníkov mobilných i pevných sietí. To umožňuje poskytovateľom služieb použiť konkrétne služby, ktoré môže dané zariadenie (mobil, PC, IP telefón, atď.) spracovať [36].



Obr. 1.1: IMS vrstvový model [36].

1.4 IMS Core prvky

1.4.1 Call Session Control Function (CSCF)

Call Session Control Function (CSCF) vytvára, monitoruje a poskytuje pomocné funkcie potrebné pri nadväzovaní multimediálnych spojení. CSCF riadi prístupové služby užívateľov. CSCF môže pracovať ako *Proxy CSCF* (P-CSCF), *Serving CSCF* (S-CSCF), *Interrogating CSCF* (I-CSCF) a *Emergency CSCF* (E-CSCF). Spoločným znakom CSCF je, že plnia dôležitú úlohu počas prihlasovania užívateľa a nadväzovania spojenia. Vytvárajú SIP spojenia a prenesené dáta sú poslané k offline spoplatneniu (*angl. offline charging*). P-CSCF a S-CSCF umožňujú ukončiť spojenie na žiadosť užívateľa. P-CSCF a S-CSCF sú schopné skontrolovať obsah (SDP) Session

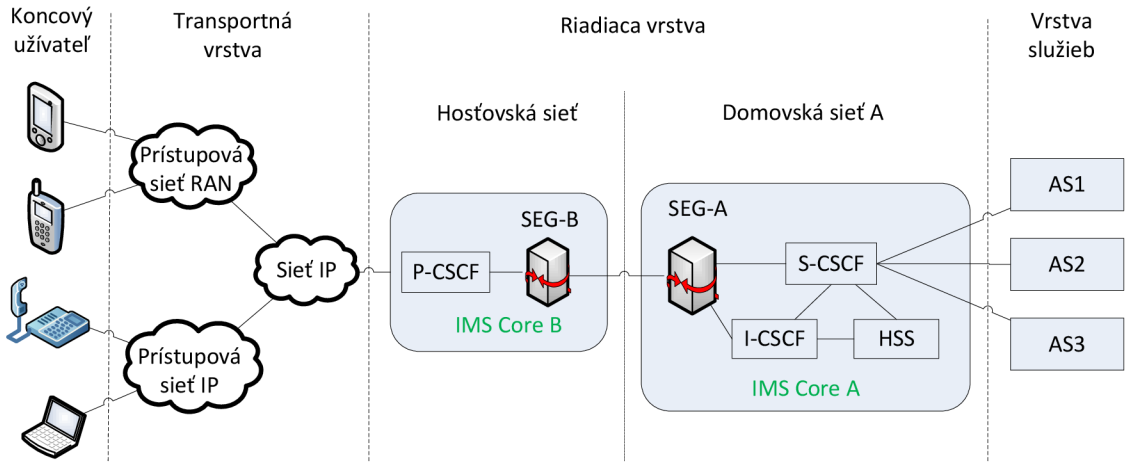
Description Protokolu. Na základe analýzy SDP dát môžu určiť, aké typy dát (multimediálne správy, video, ...) prijímajú konkrétni užívatelia [36].

1.4.2 Proxy Call Session Control Function (P-CSCF)

P-CSCF slúži ako prvý kontaktný bod medzi užívateľom a IMS subsystémom. To znamená, že všetky SIP signalizačné dáta od UE budú poslané práve do P-CSCF. P-CSCF plní *štyri základné úlohy* [36]:

- kompresiu SIP dát,
- komunikáciu s PDF (Policy Decision Function),
- asociáciu s IPsec (Internet Protocol security),
- a detekciu tiesňového volania (*angl. emergency session detection*).

SIP protokol je textovo orientovaný signalizačný protokol, ktorý obsahuje veľké množstvo hlavičiek a parametrov vrátane rozšírení a zabezpečovacích informácií [36]. Všetky tieto informácie zväčšujú veľkosť SIP správ, ktoré sú v konečnom dôsledku väčšie ako binárne kódované (*angl. binary-encoded*) protokoly. 3GPP pre zrýchlenie zostavenia relácie vyžaduje kompresiu SIP správ medzi UE a P-CSCF. Ak UE požaduje prijať komprimovanú SIP správu, P-CSCF musí túto kompresiu vykonať. Na obrázku 1.2 je zobrazená architektúra NGN siete z pohľadu vrstvového modelu.



Obr. 1.2: IMS Sieť budúcej generácie NGN (Next Generation Network) [46].

P-CSCF zodpovedá za vytvorenie relácie a prenos informácií do PDF, ak chce operátor použiť SBLP (Service-Based Local Policy). SBLP sa používa ako synonymum pre označenie IP policy control v IMS subsystéme. SBLP slúži na zaistenie kvality spojenia v IMS subsystéme. Na základe prijatej informácie je PDF schopné odvodiť IP QoS (Quality of Service) informácie, ktoré budú poslané do GGSN (Gateway GPRS Support Node) [36].

P-CSCF je zodpovedné za udržiavanie bezpečnostných asociácií SAs (*angl. Security Associations*), dodržiavanie integrity a bezpečnosti pre SIP signalizáciu počas SIP prihlasovania pri vyjednávaní IPSec bezpečnostných asociácií medzi UE a P-CSCF. Po uskutočnení prihlásenia je P-CSCF schopné aplikovať bezpečnostné opatrenia pre SIP signalizáciu. IMS sieť detekuje núdzové pokusy o nadviazanie spojenia a vedie UMTS UE k použitiu okruhovo prepínanej siete CS (Circuit Switched) pre zostavenie núdzového spojenia. Táto detekcia je úlohou P-CSCF [36].

1.4.3 Serving Call Session Control Function (S-CSCF)

S-CSCF patrí medzi hlavné prvky IMS subsystému a zodpovedná za spravovanie prihlasovacieho procesu, rozhodovanie pri smerovaní, správu relačných stavov a ukladanie profilov služieb. Ak užívateľ odošle požiadavku na prihlásenie, tak bude smerovaná z S-CSCF. S-CSCF následne stiahne autentizačné dáta z databázy účastníkov HSS (Home Subscriber Server). Na základe autentizačných dát vytvorí výzvu (*angl. challenge*) pre UE. Po prijatí odpovede a overení, S-CSCF prijme požiadavku na prihlásenie a začne spravovať stav relácie. Po ukončení tejto procedúry môže užívateľ prijímať IMS služby. S-CSCF si stiahne profil dostupných služieb z HSS ako súčasť prihlasovacieho procesu [36].

V databáze účastníkov (HSS) sú trvalo uložené jednotlivé nastavenia servisných profilov pre účastníkov danej siete konkrétneho operátora. S-CSCF si tieto servisné profily sťahuje a prideľuje ich užívateľom (*napr. michal.novy@ims.priklad.sk*). S-CSCF využíva informácie, ktoré sú zahrnuté v servisnom profile pri rozhodovaní kedy, a hlavne ktorý aplikačný server je kontaktovaný, keď užívateľ odošle SIP požiadavku, alebo prijme požiadavku od niekoho iného. Servisný profil môže obsahovať ďalšie informácie o tom, aký druh media policy musí S-CSCF aplikovať. Napríklad: servisný profil môže dovoľovať použiť užívateľovi iba zvukové aplikácie, ale nie je mu povolený prístup k video službám [36].

Jednou z funkcií S-CSCF je správa smerovania. S-CSCF prijíma všetky požiadavky na zostavenie i zrušenie spojenia od UE. Keď S-CSCF príjme od UE požiadavku na zostavenie spojenia cez P-CSCF, musí určiť, či majú byť prioritne kontaktované

aplikačné servery AS (Application Servers), aby bolo možné poslať požiadavku ďalej. Po kontaktovaní aplikačného serveru, S-CSCF pokračuje v IMS spojení, alebo predá reláciu inej CS doméne, alebo ďalšej IP sieti. Ak UE používa MSISDN (Mobile Subscriber International ISDN Number) číslo na kontaktovanie volaného účastníka, tak S-CSCF konvertuje MSISDN číslo na SIP URI (Universal Resource Identifier) formát a prioritne odošle požiadavku ďalej, pretože IMS nesmeruje požiadavky na základe MSISDN čísel. I keď S-CSCF pozná všetky IP adresy UE získané pri prihlasovacom procese, všetky požiadavky smeruje na P-CSCF, keďže P-CSCF sa stará o všetku SIP kompresiu a bezpečnostné aspekty [36].

1.4.4 Interrogating Call Session Control Function (I-CSCF)

I-CSCF je kontaktný bod u poskytovateľa siete (operátorom) pre všetky prepojenia smerujúce k predplatiteľovi služieb. I-CSCF vykonáva štyri dôležité funkcie: [36]

- Získava meno ďalšieho skoku (*angl. next hop*), (či už je to S-CSCF, alebo aplikačný server) z databázy účastníkov (HSS).
- Priraďuje S-CSCF na základe vlastností zistených z HSS. Priradenie nastáva vtedy, keď sa užívateľ prihlasuje do siete, alebo prijíma SIP požiadavku.
- Sieťovanie vstupných požiadaviek k priradenému S-CSCF, alebo aplikačnému serveru.
- Poskytovanie Topology Hiding Inter-network Gateway (THIG) funkcionality. THIG môže byť použitá na skrývanie konfigurácií, kapacity a topológie mimo operátorovej siete.

1.4.5 Emergency Call Session Control Function (E-CSCF)

Pre tiesňové volania v IMS subsystéme slúži E-CSCF entita, ktorá obsluhuje požiadavky pre vytvorenie hovoru pre políciu, hasičov a lekársku pohotovosť. Hlavnou úlohou E-CSCF je výber pohotovostného centra PSAP (Public Safety Answering Point), kam sú smerované všetky tiesňové hovory. Ak užívateľ uskutoční núdzový hovor, hlavným požiadavkom je informácia o polohe užívateľa a možný druh pohotovostnej služby (napr. polícia, hasičská služba, atď.). Po zvolení správneho pohotovostného centra, E-CSCF presmeruje požiadavku na zvolené pohotovostné centrum. [36].

1.5 Databázy

V IMS subsystéme sa vyskytujú dva druhy databáz: databáza účastníkov HSS (Home Subscriber Server) a databáza SLF (Subscription Locator Function) [36].

1.5.1 Home Subscriber Server (HSS)

V HSS sú uložené všetky dáta týkajúce sa užívateľov a služieb, ktoré poskytuje IMS. Domovská sieť môže obsahovať jednu, alebo niekoľko HSS databáz v závislosti na počte užívateľov, kapacite zariadenia a organizácie siete. HSS zodpovedá za uloženie informácií týkajúcich sa: [36]

- Identifikácie o užívateľoch, číslovaní a informácie o adresovaní.
- Bezpečnostné informácie o užívateľoch: autentizácia a autorizácia pre prístup užívateľov do IMS subsystému.
- Informácie o polohe užívateľov v rámci vnútorného systému: HSS podporuje prihlasovanie užívateľov a ukladá informácie o ich polohe v rámci vnútorného systému.
- Používateľské profily.

HSS rieši autentizáciu, autorizáciu, adresovanie, lokalizáciu atď. HSS taktiež generuje bezpečnostné informácie užívateľov pre vzájomnú autentiáciu, zaistenie integrity a šifrovanie. Identita užívateľa sa skladá zo súkromnej (*angl. private*) a verejnej (*angl. public*) identity. Súkromná identita je identita užívateľa, ktorá je užívateľovi priradená operátorom v domácej sieti a používa sa za účelom prihlásenia a autorizácie, zatiaľ čo verejná identita je identita, ktorú môžu ostatní užívatelia použiť pre vyžiadanie komunikácie s koncovými užívateľmi. Informácie o aktivácii služieb (*angl. service-triggering information*) umožňujú spustenie SIP služieb.

HSS poskytuje pre S-CSCF špeciálne informácie o užívateľoch. Tieto informácie následne požíva I-CSCF na výber najvhodnejšieho S-CSCF. Z ďalších funkcií, ktoré sú zahrnuté v IMS subsystéme a obsahuje ich HSS databáza je to domáci lokačný register HLR (Home Location Register) a Autentizačné centrum AuC (Authentication Center), ktoré sú potrebné pre paketovo orientovanú sieť PS (Packet-Switched) a sieť s prepínaním okruhov CS (Circuit-Switched) [5], [36].

Domáci lokačný register (HLR)

Funkcia HLR registra je vyžadovaná z dôvodu podpory SGSN (Serving GPRS Support Node) a GGSN (Gateway GPRS Support Node) v paketovo orientovanej sieti, ktoré umožňujú užívateľom prístup k službám paketovej siete. HLR takisto poskytuje podporné funkcie pre MSC/MSC servery, ktoré sa nachádzajú v okruhovo prepínaných sieťach. To umožňuje užívateľom prístup k službám CS domény a podporu roamingu v (GSM)/UMTS okruhovo prepínaných sieťach [36].

Autentizačné centrum (AuC)

V AuC je uložený unikátny tajný kľúč pre každého mobilného účastníka, ktorý sa používa na generovanie dynamicky zabezpečených dát každého mobilného účastníka. Tieto dáta sú potom používané na vzájomnú autentizáciu IMSI (International Mobile Subscriber Identity) a mobilnej siete. Takto zabezpečené dáta sa používajú na zaistenie integrity a šifrovanie komunikácie v rádiovom spektre medzi UE a mobilnou sieťou [36].

1.5.2 Subscription Locator Function (SLF)

SLF sa používa ako rozlišovací mechanizmus, ktorý umožňuje I-CSCF, S-CSCF a AS nájsť adresu HSS databázy. Databáza obsahuje užívateľské dáta a jeho identifikačné prvky v prípade, že sú použité viaceré samostatne adresované HSS databázy [5], [36].

1.6 Rozhrania v IMS

Komunikácia medzi jednotlivými prvkami v IMS subsystéme je zabezpečená pomocou komunikačných protokolov, medzi ktoré patria napríklad: SIP (Gm, Ici, ICS, Ix, Mg, Mi, Mj, Mk, Mr, Mw, Mx, Rc), DIAMETER (Cx, Dh, Dx, Sh), H.248 (Mn, Mp), HTTP/XCAP (Ut), RTP (Izi) a MAP (Si). Všetky rozhrania sú zobrazené v prílohe na obrázku A.1.

Cr rozhranie

Cr rozhranie umožňuje komunikáciu pomocou protokolu DIAMETER medzi aplikačným serverom (AS) a MRFC (Media Resource Function Controller). Cr referenčný bod poskytuje pre MRFC možnosť získať dokumenty a zdroje z aplikačného servera a spracované dáta vrátiť naspäť do AS.

Cx rozhranie

Cx rozhranie slúži na prenos informácií o užívateľoch, ktoré sú uložené v HSS. Tieto informácie používajú I-CSCF a S-CSCF pri prihlasovaní užívateľov. Ako komunikačný protokol je použitý protokol DIAMETER.

Dh rozhranie

Rozhranie Dh sa nachádza medzi aplikačným serverom AS a SLF. Rozhranie Dh nie je potrebné, ak v sieti existuje iba jedno HSS. Ak je v sieti použitých viacero

HSS, Dh rozhranie sa používa ako referenčný bod pre kontaktovanie SLF aplikačným serverom AS. Ako komunikačný protokol je použitý protokol DIAMETER.

Dx rozhranie

Rozhranie Dx poskytuje komunikáciu medzi SLF a I-CSCF. Protokol DIAMETER je použitý na zaistenie tejto komunikácie. Rozhranie Dx sa používa v prípade, že sa v sieti vyskytuje viacero HSS. I-CSCF a S-CSCF pri výskyte viacerých HSS nevedia, ktoré HSS musia kontaktovať. Z toho dôvodu najskôr kontaktujú SFC, ktorá pomocou vyhľadávacieho mechanizmu nájde adresu HSS s profilom hľadaného užívateľa. Referenčný bod Dx je vždy v spojení s referenčným bodom Cx.

Gm rozhranie

Gm rozhranie je referenčný bod, ktorý sa nachádza medzi P-CSCF a UE. Pre signalizáciu je použitý SIP protokol. Na rozhraní môžu prebiehať tri druhy aktivít: *dohľad nad reláciou*, *prihlasovanie* a *transakcie*. Pri prihlasovaní odosiela UE k P-CSCF informácie potrebné na zaistenie autentizácie pomocou SIP protokolu. Týmto procesom sa začína komunikácia medzi UE a IMS.

Ici rozhranie

Ici referenčný bod je vstupno-výstupným bodom medzi IBCF a IBCF umiestnenom v druhej IMS sieti. Na komunikačnom rozhraní Ici pracuje SIP protokol.

ISC (IMS Service Control Reference Point) rozhranie

ISC rozhranie slúži ako referenčný bod medzi S-CSCF a aplikačným serverom, po ktorom sa posielajú SIP správy pomocou SIP protokolu. ISC procedúry možno rozdeliť na dve hlavné kategórie: smerovanie počiatočnej SIP správy do AS a SIP požiadavky generované AS a odosielané k S-CSCF.

Ix rozhranie

Referenčný bod Ix umožňuje IBCF ovládať TrGW (Transition Gateway) pomocou SIP protokolu. TrGW podporuje kontrolu média, označovanie paketov na základe QoS, prideľovanie šírky pásma, a ďalšie funkcie. Všetka komunikácia medzi TrGW a IBCF je zabezpečená cez Ix rozhranie.

Izi rozhranie

Izi referenčný bod slúži ako spojovací bod medzi TrGW jedného IMS subsystému a druhým TrGW iného IMS subsystému. Po rozhraní Izi, TrGW preposiela multimediálny obsah medzi jednotlivými IMS sieťami k ďalším TrGW. Izi rozhranie pracuje na RTP (Real-time Transport Protocol) protokole.

Mg rozhranie

Entity MGCF (Media Gateway Controller Function) a I-CSCF spája rozhranie Mg. Komunikácia je zaistená pomocou SIP protokolu. Rozhranie umožňuje posielanie signalizácie MGCF entite z CS domény do I-CSCF.

Mi rozhranie

Mi referenčný bod sa nachádza medzi S-CSCF a BGCF (Breakout Gateway Control Function). Ako komunikačný protokol je použitý SIP protokol. Mi rozhranie sa využíva na smerovanie relácie z S-CSCF, alebo E-CSCF do CS domény.

Mj rozhranie

Mj rozhranie sa využíva na preposielanie relácie z BGCF do MGCF v prípade, že nastane prerušenie relácie. Mj referenčný bod je umiestnený medzi MGCF a BGCF a na komunikáciu využíva SIP protokol.

Mk rozhranie

Mk referenčný bod je umiestnený medzi BGCF a ostatnými IMS sieťami. Mk rozhranie sa využíva na preposielanie signalizácie z BGCF do ostatných IMS sietí v prípade, že BGCF obdrží požiadavku o reláciu pre CS doménu, ktorá sa nenachádza v danej domovskej sieti. Pre komunikáciu je využívaný SIP protokol.

Mn rozhranie

Mn rozhranie slúži na zaistenie komunikácie s ostatnými multimediálnymi IP sieťami v IMS subsystéme. Mn referenčný bod umožňuje I-CSCF prijímať požiadavky o spojenie zo SIP serverov alebo terminálov. Mn rozhranie je založené na H.248 odporúčaní [13], ktoré je určené pre audiovizuálne a multimediálne systémy.

Mr rozhranie

Mr referenčný bod sa používa ako komunikačné rozhranie medzi MRFC a S-CSCF v IMS subsystéme. Na komunikáciu sa používa SIP protokol. Mr rozhranie nie je štandardizované.

Mp rozhranie

Entity MRFC a MRFP (Media Resource Function Processor) sú spojené pomocou Mp rozhrania. Na komunikáciu sa používa H.248.1 protokol, ktorý je definovaný v ITU-T (ITU Telecommunication Standardization Sector) H.248.1 [13].

Mw rozhranie

Komunikácia medzi I-CSCF/S-CSCF a P-CSCF prebieha na základe SIP protokolu po rozhraní Mw. Procedúry vykonávané na rozhraní Mw možno podobne ako procedúry vykonávané na rozhraní Gm rozdeliť do troch kategórií: *prihlasovanie*, *dohľad nad reláciou* a *transakcie*. Pri prihlásení zašle P-CSCF požiadavku k I-CSCF, ktorý ju spracuje a odošle k správnemu S-CSCF. Po spracovaní žiadosti odošle S-CSCF odpoveď priamo k P-CSCF po Mw rozhraní.

Mx rozhranie

Mx referenčný bod pracuje pracuje na SIP protokole. Používa sa na prenos informácií medzi IBCF a BGCF, prípadne I-CSCF.

Rc rozhranie

Rc rozhranie sa nachádza medzi MRB (Media Resource Broker) a aplikačným serverom (AS). AS používa Rc rozhranie pri žiadosti o priradenie šírky pásma pre hovor od MRB. MBR môže pracovať v *In-Line*, alebo v *Query* móde [3].

Sh rozhranie

Rozhranie Sh poskytuje komunikačné rozhranie medzi AS a HSS. Ak AS (SIP AS, alebo OSA SCS) potrebuje dáta (týkajúce sa identity užívateľa), alebo potrebuje zistiť ku ktorému S-CSCF má poslať SIP požiadavku, použije Sh referenčný bod a získa potrebné údaje z HSS. Komunikačný protokol použitý na rozhraní Sh je DIAMETER. Procedúry na tomto rozhraní sa delia na dve kategórie: správu dát a predplatné/upozornenia (*angl. subscription/notification*).

Si rozhranie

Rovnako ako pri rozhraní Sh, je rozhranie Si umiestnené medzi AS a HSS. Tento referenčný bod slúži na výmenu informácií medzi IM-SSF AS (používa CAMEL platformu) a HSS. Komunikácia funguje na MAP (Mobile Application Part) protokole.

Ut rozhranie

Ut rozhranie sa používa ako referenčný bod medzi UE a AS. Na rozhraní prebieha komunikácia prostredníctvom HTTP (Hyper Text Transfer Protocol) protokolu. To umožňuje užívateľom bezpečne spravovať a konfigurovať svoje sieťové služby, ktoré sú umiestené na AS. [36].

2 IMS PROTOKOLY

V IP Multimedia Subsystem pracuje veľké množstvo protokolov. Medzi hlavné signalizačné protokoly, ktoré sa využívajú v IMS subsystéme patria SIP (Session Initiation Protocol) a DIAMTER. SIP protokol slúži k zostaveniu, prípadne ukončeniu relácie medzi dvoma, alebo viacero klientami v IP sieťach [36]. Okrem týchto dvoch hlavných protokolov sa IMS sieti používajú aj iné protokoly. Napríklad: DNS (Domain Name System), RTP, SDP (Session Description Protocol), TLS (Transport Layer Security), HTTP (Hyper Text Transfer Protocol), SNMP (Simple Network Management Protocol) a iné.

2.1 SIP (Session Initiation Protocol)

SIP protokol je signalizačný protokol pracujúci na aplikačnej vrstve, vyvinutý organizáciou IETF (Internet Engineering Task Force). V roku 2002 bol SIP protokol publikovaný v RFC 3261 [38]. Protokol je určený pre vytváranie, modifikovanie a ukončenie multimediálnych relácií s jedným, alebo viacerými koncovými bodmi za účelom zostavenia telefónnych hovorov, video hovorov, videokonferencií, instant messaging-u (IM), multimediálneho dátového toku, online hier a podobne.

SIP protokol je nezávislý na transportnej vrstve a SIP komunikácia je tvorená pomocou správ, ktoré sú posielané medzi SIP zariadeniami pomocou UDP (User Datagram Protocol) a TCP (Transmission Control Protocol), alebo iného transportného protokolu. Na prenos multimediálnych dát v reálnom čase sa SIP protokol najčastejšie používa v kombinácii s RTP protokolom. SDP protokol, ktorý sa používa na popis multimediálnych relácií umožňuje účastníkom dohodnúť sa na množine parametrov, ktoré sú potrebné pre zostavenie multimediálnej komunikácie. SDP popis môže byť zahrnutý práve v SIP správach. SIP taktiež spolupracuje s množstvom iných protokolov [38].

SIP záhlavie

SIP komunikácia je založená na výmene SIP správ, zabezpečených transportným protokolom. Rozlišujeme dva druhy SIP správ, a to SIP požiadavky (*angl. requests*) a SIP odpovede (*angl. responses*).

SIP požiadavky

Záhlavie SIP požiadavky obsahuje tri základné údaje: typ metódy (*angl. Method name*), URI adresu (*angl. Request-URI*) a verziu SIP protokolu (*angl. SIP version*).

RFC 3261 [38] definuje šesť hlavných metód používaných v SIP protokole: ACK, BYE, CANCEL, INVITE, REGISTER a OPTIONS.

SIP protokol taktiež obsahuje aj niekoľko ďalších rozširujúcich metód: UPDATE, INFO, PUBLISH, MESSAGE, NOTIFY a SUBSCRIBE. V kapitole 2.1.2 sú podrobnejšie opísané hore uvedené metódy. URI adresa sa vyskytuje ako druhá položka v záhlaví SIP požiadavky. URI adresa predstavuje SIP URL (Uniform Resource Locator), ktorý označuje klienta, alebo server ku ktorému je SIP požiadavka smerovaná. Verzia protokolu SIP nám určuje typ použitej SIP verzie. Pre verziu 2.0 je dané označenie „SIP/2.0“.[38]

SIP odpovede

Záhlavie SIP odpovedí obsahuje informácie týkajúce sa verzie protokolu (*angl. SIP version*), kódu odpovede (*angl. Status code*) a samotného textu odpovede (*angl. Reason phrase*). Verzia protokolu uvedená v záhlaví SIP odpovede musí byť rovnaká s verziou protokolu uvedenou v záhlaví SIP požiadavky. Kód odpovede predstavuje trojčíselný kód vo formáte (XYZ), pomocou ktorého sa vyjadruje odpoveď na SIP požiadavku. Podrobnejší popis jednotlivých číselných kombinácií je uvedený v kapitole 2.1.3. Text odpovede uvádza slovný popis číselného kódu (XYZ) [37].

2.1.1 SIP hlavičky

Každá SIP požiadavka a taktiež každá SIP odpoveď musí obsahovať sedem povinných hlavičiek. Medzi tieto hlavičky patrí: Call-ID, Contact, CSeq, From, To, Max-Forwards a Via. Okrem povinných hlavičiek existuje ešte veľa nepovinných hlavičiek, napr. Accept, Authorization, Contact-Type, Date, Event, Route, Subject a mnohé iné [37].

Contact

Hlavička Contact poskytuje informácie o adrese účastníka SIP relácie. Je to zoznam SIP adries, ktoré môže daný klient používať. Ak je adries v zozname uvedených viac, najvyššiu prioritu má posledná adresa.
Zápis hlavičky: Contact: <sip:svec@stud.feec.vutbr.cz>.

CSeq

Jednoznačne daný identifikátor žiadosti v rámci jednej relácie nám udáva CSeq hlavička. V prípade, že neprišla žiadna odpoveď na SIP požiadavku a žiadosť sa opakuje, má Cseq rovnaké číslo.
Zápis hlavičky: CSeq: 4711 INVITE.

From

Hlavička From identifikuje iniciátora SIP požiadavky. Hlavička From môže byť rovnaká, ak sú zhodné URI identifikátory a ich parametre.
Zápis hlavičky: FROM: "Jan Svec" <sip:sv23@feec.vutbr.cz>; tag=a48s-54d.

To

Hlavička To je logicky členená na tri časti. Prvá časť hlavičky obsahuje meno klienta, ktoré je možné zobraziť na displeji koncových zariadení. Druhá časť hlavičky, ktorá je ohraničená znakmi „<“ a „>“ je reálna adresa klienta. Tretia časť hlavičky „tag“ sa používa pri testovaní dialógu. Dialóg je kombináciou Call-ID spolu s dvoma tagmi, každý od jedného účastníka dialógu.
Zápis hlavičky: TO: "Michal Svec" <sip:sv2@stud.feec.vutbr.cz>; tag=a48s.

Max-Forwards

Ako prevencia proti zacykleniu sa používa hlavička Max-Forwards. Hlavička je pri vytvorení inicializovaná na počiatočnú hodnotu (70), ktorá sa pri prechádzaní sieťou postupne znižuje až na minimálnu hodnotu 0. Ak je dosiahnutá hodnota 0, správa sa automaticky zahodí.
Zápis hlavičky: Max-Forwards: 55.

Via

V hlavičke Via sa ukladá cesta SIP správy. Pri postupnom prechode správy cez jednotlivé proxy servery v sieti, pridá každý proxy server na začiatok hlavičky Via svoju adresu a dodatočne kontroluje, či adresa na ktorú chce správu preposlať je už obsiahnutá v hlavičke. Tento proces bráni opätovnému preposlaniu správy serveru, ktorý už SIP správu takto spracovával. Pri spätnej odpovedi server vymaže zo správy svoju adresu.
Zápis hlavičky: Via: SIP/2.0/UDP feec.vutbr.cz:5060; branch=z9hG4bK98ks7.

Telo SIP správy

V tele SIP správy (*angl. Optional Message Body*) sa môže vyskytovať akákoľvek informácia. V SIP pakete môžu byť zapuzdrené aj dáta iného protokolu. Najčastejšie sa do SIP správ zapuzdrujú dáta SDP protokolu, ktorý popisuje detailné vlastnosti pri zahájení relácie [37].

2.1.2 SIP metódy

Existuje šesť hlavných SIP metód. Nižšie je uvedený stručný prehľad hlavných SIP metód s popisom ďalších vybraných metód.

ACK

Metóda ACK sa používa na potvrdzovanie žiadostí pre spojenie INVITE. Spojenie sa nadviaže len vtedy, ak zdroj, ktorý odosiela INVITE metódu, prijme od adresáta metódu ACK. Ak nastane situácia pri ktorej odosielateľ prijme viac týchto odpovedí (konferenčné hovory), musí odoslať ACK každému zariadeniu, od ktorého prijal odpoveď.

BYE

Metóda BYE sa používa pri ukončovaní relácie.

CANCEL

Pre zrušenie žiadosti, ešte pred potvrdením žiadosti od cieľového adresáta sa používa metóda CANCEL. Ak sa užívateľ pokúša o spojenie, napríklad z mobilného telefónu (pomocou metódy INVITE) a ešte pred spojením hovoru (vyzváňanie), užívateľ hovor ukončí, posiela sa metóda CANCEL. CANCEL metóda však môže byť prijatá aj po spracovaní metódy INVITE. V takom prípade bude odpoveď ignorovaná.

INVITE

Metóda INVITE sa používa na nadviazanie relácie, alebo aj ako žiadosť o zmenu parametrov už vytvorenej relácie, v rámci IMS subsystému.

OPTIONS

Pre zasielanie informácií o službách podporovaných na serveri sa používa práve metóda OPTIONS. V prijatej odpovedi sú obsiahnuté všetky funkcie, ktoré poskytuje dané zariadenie (entita). Prijatá odpoveď obsahuje ACCEPT hlavičku.

SUBSCRIBE

Ak aplikačný server (AS) žiada obnovenie informácií z S-CSCF a HSS, použije sa metóda SUBSCRIBE. Napríklad pre zistenie dostupnosti určitých klientov v IMS sieti sa použije metóda SUBSCRIBE. S-CSCF odpovedá na metódu SUBSCRIBE správou NOTIFY.

NOTIFY

S-CSCF používa metódu NOTIFY k informovaniu AS. NOTIFY metóda obsahuje zmeny, ktoré boli vykonané počas novej registrácie.

UPDATE

UPDATE metóda sa používa pre aktualizáciu informácií o relácii. Je definovaná v RFC 3311 [41]. UPDATE správy obsahujú informácie o zmenených parametroch spojenia prostredníctvom SDP.

2.1.3 SIP odpovede

SIP odpovede sú odpoveďami na SIP žiadosti. Kódy SIP odpovedí sa vyskytujú v číselnom formáte v rozsahu od 100 do 699. Odpovede od čísla 200 vyššie sú konečnými odpoveďami. SIP odpovede sa delia do šiestich tried začínajúcich prvou číslicou v trojcifernom značení. Ďalšie dve číslice presnejšie určujú stav danej triedy [37].

1xx

Informačné odpovede (*angl. Provisional Responses*) oznamujú, že žiadosť bola prijatá a je v stave spracovania. Odpovede sú zasielané z proxy servera, alebo z presmerovávacieho (*angl. Redirect*) servera.
Formát odpovede: 100 Trying, 180 Ringing, 181 Call is Being Forwarded.

2xx

Úspešné vykonanie žiadosti (*angl. Successful Response*) oznamuje o tom, že žiadosť bola úspešne spracovaná. Napríklad označenie „202 Accepted“ oznamuje, že požiadavka bola prijatá na spracovanie, ale žiadosť ešte nebola spracovaná.
Formát odpovede: 200 OK, 202 Accepted, 204 No Notification.

3xx

Pomocou presmerovacích serverov sú posielané odpovede na presmerovanie (*angl. Redirection Response*). Obvykle sú to odpovede s informáciami o lokalizácii klienta, alebo o alternatívnej službe.
Formát odpovede: 300 Multiple Choices, 301 Moved Permanently.

4xx

Ak sa vyskytne chyba na strane klienta (*angl. Client Failure Response*), táto skutočnosť je oznámená pomocou chybovej odpovede. Odpoveď indikuje chybu, ktorou

môže byť napríklad nesprávna syntax žiadosti a žiadosť tak nemôže byť vykonaná.
Formát odpovede: 400 Bad Request, 401 Unauthorized, 403 Forbiden.

5xx

Pomocou číselnej kombinácie „5xx“ sa označuje chyba, ktorá nastala na strane servera (*angl. Server Failure Response*). Táto odpoveď oznamuje klientovi, že žiadosť je síce správna, ale server, ktorý žiadosť spracovával zlyhal.
Formát odpovede: 500 Server Internal Error, 502 Bad Gateway.

6xx

Odpoveď na požiadavku, ktorú nie je možne vykonať na žiadanom serveri. Poskytuje odpoveď s kódovým označením „6xx“ typu globálna chyba (*angl. Global Failure Response*).
Formát odpovede: 600 Busy Everywhere, 603 Decline, 606 Not Acceptable.

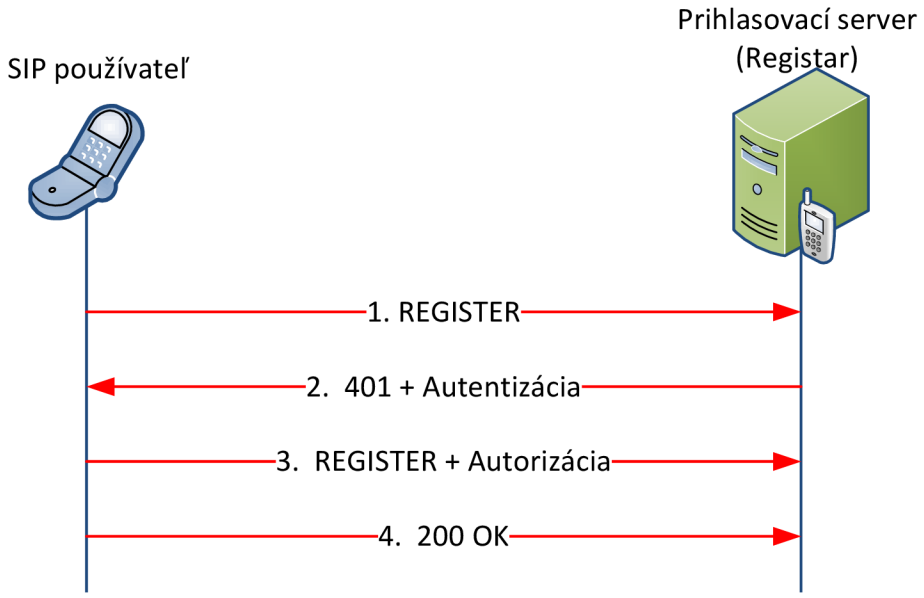
2.1.4 SIP prihlasovanie

Aby bol užívateľ dostupný pre všetkých klientov, musí sa najskôr prihlásiť na prezenčnom serveri pomocou správy REGISTER. Prihlásenie pozostáva z požiadavky REGISTER a odpovede na požiadavku „200 OK“. Prihlásenie však môže byť aj neoprávnené, táto skutočnosť je potom oznámená klientovi pomocou negatívnej odpovede označenej kódom 401 (Unauthorized), alebo 407 (Proxy Authentication Required) [38].

Ak klient obdrží odpoveď označenú kódom 401, znamená to, že klient nevyplnil potrebné údaje nutné k prihláseniu. Odpoveď obsahuje hlavičku WWW Authenticate s výzvou doplnenia údajov pre úspešné prihlásenie. Užívateľ je prihlásený v prípade, že zopakuje požiadavku na prihlásenie so správne vyplnenými údajmi vo výzve *Authorization*. Priebeh prihlasovania je znázornený na obrázku 2.1.

2.2 DIAMETER

Protokol DIAMETER patrí medzi tzv. AAA (Authentication, Authorization and Accounting) protokoly, medzi ktoré patria aj protokoly TACACS (Terminal Access Controller Access-Control System) a RADIUS (Remote Authentication Dial In User Service). Tieto protokoly sa požívajú na vzdialený prístup do sietí. Protokol RADIUS bol predchodcom protokolu DIAMETER. Hlavným rozdielom protokolu



Obr. 2.1: Priebeh SIP prihlásenia [50].

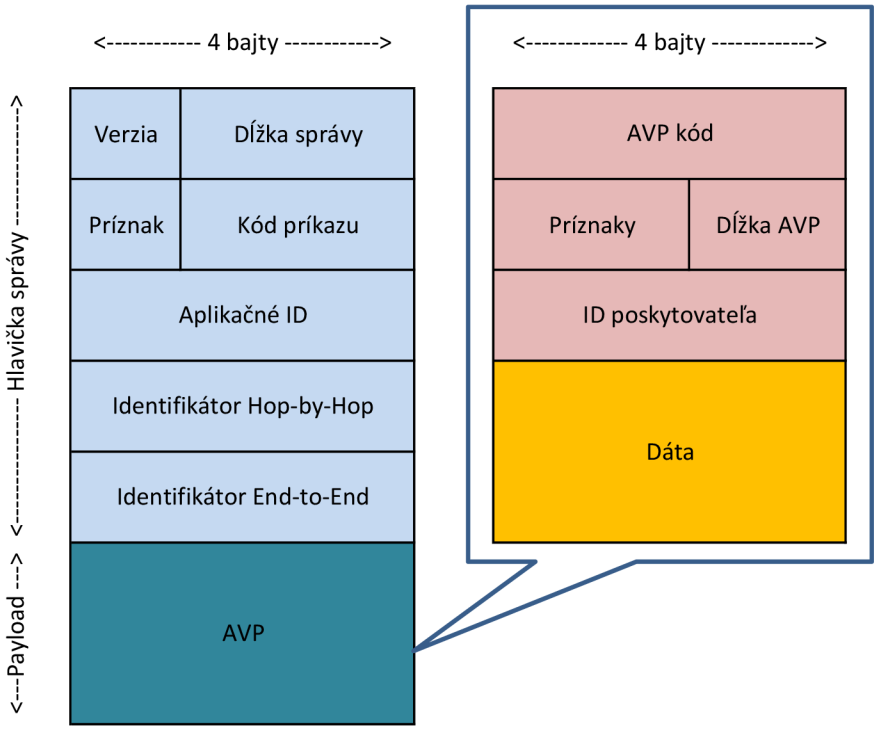
DIAMETER oproti svojmu predchodcovi je, že DIAMETER používa na prenos údajov spoľahlivé transportné protokoly TCP a SCTP (Stream Control Transmission Protocol). RADIUS používa na prenos údajov UDP protokol, ktorý patrí medzi nespoľahlivé transportné protokoly [10]. Na prenos zabezpečených správ požíva zabezpečenie pomocou IPSec alebo TLS protokolom [42].

Protokol DIAMETER definuje tri typy prvkov: klient, server a agent. Agentov môže byť niekoľko druhov: *relay agent*, *proxy agent*, *redirect agent* a *translation agent*. Vzťahy medi agentmi a ich stručný popis možno nájsť na [19].

Formát paketu protokolu DIAMTER pozostáva z hlavičky protokolu a niekoľkých AVP (Attribute-Value Pairs), ktoré slúžia na prenos dát. AVP prenášajú dáta a informácie týkajúce sa smerovania, kapacity, AAA a bezpečnosti medzi dvoma DIAMETER prvkami. Kódom príznaku sa určuje typ správy. Napríklad príznakom R (Request) možno bitovým nastavením určiť, či sa jedná o požiadavku (*angl. request*), alebo o odpoveď [19]. DIAMETER paket spolu s AVP hlavičkou je zobrazený na obrázku 2.2.

2.3 SNMP

SNMP (Simple Network Management Protocol) je protokol pracujúci na aplikačnej vrstve. SNMP protokol je určený na výmenu riadiacich informácií medzi zariadeniami pracujúcimi v sieti. Použitím SNMP protokolu možno pristupovať k infor-



Obr. 2.2: Zobrazenie DIAMETER paketu a AVP hlavičky [19].

máciám ako sú napr. počet prenesených paketov za určitý čas, počet nedoručených paketov a podobne. Administrátori spravujúci sieťové prostriedky a služby môžu pomocou SNMP protokolu jednoduchšie nájsť a riešiť prípadný problém a taktiež kontrolovať stav sieťovej komunikácie [44].

2.3.1 SNMP verzia 1.0

Agenti v SNMP v.1 pracujú ako softvérové moduly na spravovaných zariadeniach. Agenti majú prístup k informáciám na spravovaných zariadeniach. Tieto informácie sú potom dostupné pre sieťový riadiaci systém NMS (Network Management System) cez SNMP v.1. Na obrázku 2.3 je grafické znázornenie riadiaceho systému [47]. SNMP protokol v.1 je definovaný v RFC 1155 [43] a 1157 [44].

Spravovaným zariadením môže byť akýkoľvek sieťový prvok vrátane serverov, tlačiarní, smerovačov a prepínačov. Dôležitým prvkom riadiaceho softvéru je, aby softvér nebol náročný na výkon hardvéru riadeného prvku (zaťaženie CPU, systémovej pamäte apod.). Spravované zariadenie môže získavať údaje o:

- počte a stave virtuálnych okruhov,

- počte prijatých chybových správ,
- počte prijatých a odoslaných bytov alebo paketov,
- maximálnej priepustnosti linky,
- prijatých a odoslaných broadcast správach,
- stave linky (výpadok, obnovenie).

Príkazy

Spravované zariadenia môžu odpovedať pomocou štyroch druhov príkazov: *Reads*, *Writes*, *Traversal operations* a *Traps*.

Reads: Používa sa na monitorovanie spravovaného zariadenia. NMS číta premenné, ktoré sú spravované daným zariadením.

Writes: Používa sa na ovládanie spravovaného zariadenia. NMS zapisuje premenné, uložené v rámci spravovaného zariadenia.

Traversal operations: NMS zistí, s ktorými premennými môže spravované zariadenie pracovať a postupne získava informácie, ktoré zapisuje do tabuliek (napr. IP smerovacia tabuľka).

Traps: Spravované zariadenia asynchrónne posielajú záznamy určitých udalostí k NMS.

MIB riadiaca databáza

Všetky spravované objekty sú uložené v riadiacej databáze MIB (Management Information Base), ktorá je v podstate databáza objektov. MIB býva popisovaná ako stromová štruktúra, ktorej listy predstavujú jednotlivé dátové prvky. Identifikátory objektov jednoznačne určujú MIB objekt v stromovej štruktúre, ktorá je hierarchicky usporiadaná. Príkladom môže byť medzinárodné telefónne číslo, ktoré sa skladá z kódu krajiny (ČR, SR, USA, ...) a telefónneho čísla konkrétneho účastníka, pridelené operátorom.

Ovládanie

SNMP v.1 je jednoduchý protokol založený na princípe výzva – odpoveď (*angl. request – response*). Sú definované štyri typy operácií.

Get: Získanie objektov od agentov.

Get-next: Získanie ďalšieho objektu z tabuľky, alebo z zoznamu v rámci agenta.

Set: Nastavenie objektov v rámci agenta.

Trap: Asynchrónne posielané informácie určitých udalostí k NMS. Narozdiel od get, get-next a set, trap nevyžaduje reakciu z prijímača.

2.3.2 SNMP verzia 2.0

SNMP verzia 2.0 je evolučnou verziou SNMP (dnes SNMP v.1). SNMP v.2 vychádza z dvoch špecifikácií: Secure SNMP a SMP (Simple Management Protocol). Secure SNMP definuje bezpečnostné prvky, ktoré nie sú dostupné v SNMP v.1 a používa typ správ, ktoré sú nekompatibilné s SNMP v.1. SMP v porovnaní s SNMP v.1 ponúka široké možnosti správy v oblasti kontroly prostriedkov, veľkosti prenášaných dát a prostredia v ktorom dokáže pracovať (TCP/IP siete). SNMP v.2 je definovaná v RFC 1902 [45].

SNMP v.2 definuje tri druhy informačných modulov:

- MIB moduly: obsahujú definície vzájomne prepojených, spravovaných objektov.
- Vyhlásenia o zhode pre MIB moduly: poskytujú popis skupiny spravovaných objektov, ktoré musia byť zhodné.
- Vyhlásenia o kompatibilite pre implementáciu agenta: definujú aký stupeň podpory má agent na spravovanom zariadení.

Ovládanie

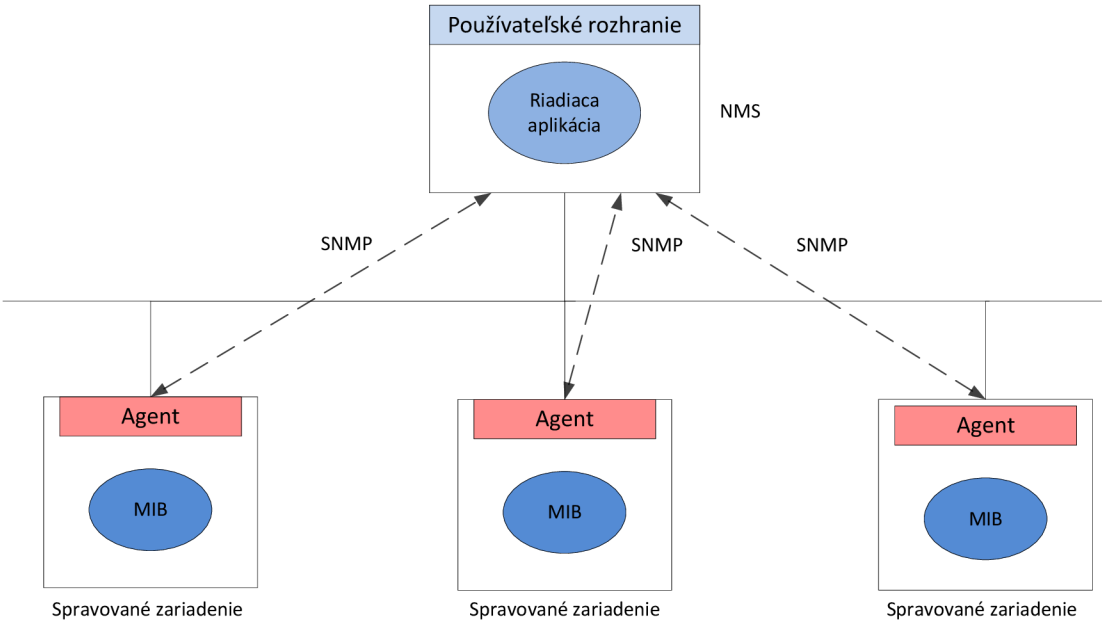
SNMP v.2 používa rovnaký druh operácií ako SNMP v.1 až na iný typ odpovedí. Okrem operácií prebratých z SNMP v.1, SNMP v.2 definuje dve nové operácie.

Inform: Umožňuje poslať trap príkaz od jedného správcu (NMS) k druhému a žiadať o odpoveď.

Get-bulk: Možnosť prijímať veľké bloky dát (viaceré riadky v tabuľke).

2.3.3 SNMP verzia 3.0

SNMP protokol verzie 3 poskytuje zabezpečený prístup k spravovaným zariadeniam pomocou autentizácie a šifrovania paketov. Výhody toho zabezpečenia spočívajú v tom, že dáta získané pomocou SNMP protokolu sú bezpečne prenášané po sieti a nikto s nimi neoprávnene nemanipuloval. Ďalšou výhodou je dôvernosť informácií. Napríklad SNMP príkazy určené na zmenu konfigurácie smerovača posielané v paketoch môžu byť šifrované a tým sa zabráni zneužitiu ich obsahu. Bezpečnostné prvky v SNMP v.3 zahŕňajú:[48]



Obr. 2.3: Riadiaci model SNMP v.1 [47].

Integritu správ: Zaručuje, že s paketom nebolo neoprávnene manipulované počas prenosu.

Autentizáciu: Potvrdzuje, že správa prišla z overeného zdroja.

Šifrovanie: Šifrovanie obsahu paketu zabraňuje jednoduchému prečítaniu obsahu paketu treťou osobou (*angl. man in the middle*).

3 IMS PROJEKTY

Existuje viacero projektov, ktoré sa zaoberajú implementáciu IMS siete. Patria medzi ne viaceré open source projekty, ale aj komerčné projekty poskytujúce platené služby. Niekoľko vybraných IMS projektov je predstavených v nasledujúcej kapitole.

3.1 Open IMS

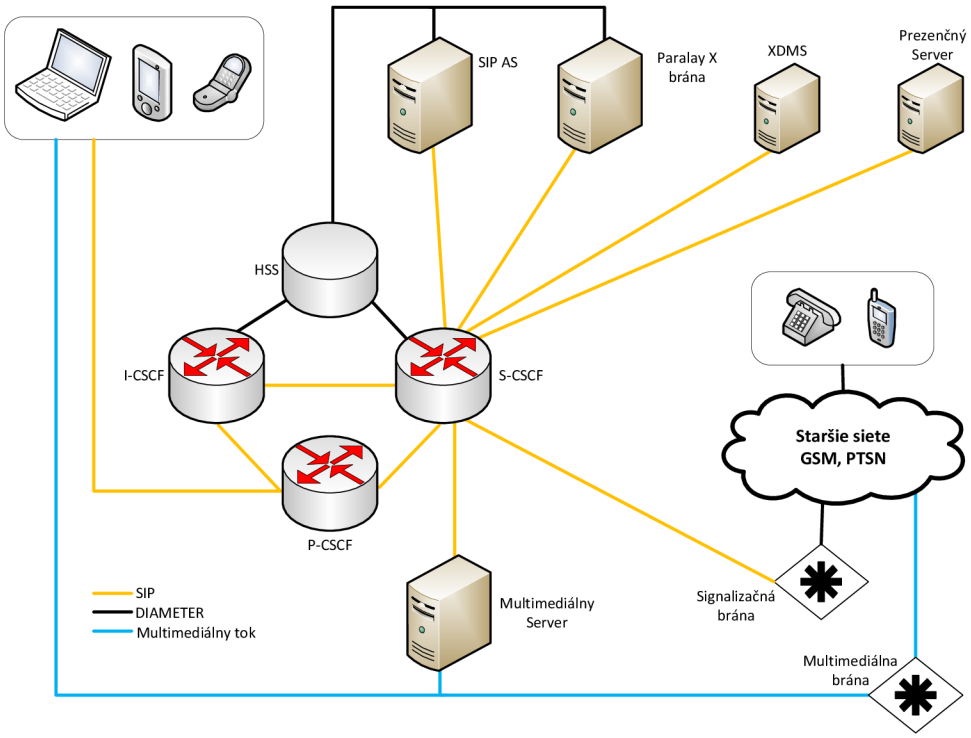
Open IMS Core je open source implementácia IMS CSCF funkcií a HSS databázy, ktoré spolu tvoria základnú architektúru IMS/NGN sietí podľa špecifikácií 3GPP, 3GPP2 a ETSI TISPAN (Telecommunications and Internet coverged Services and Protocols for Advanced Networking). Štyri základné prvky (S-CSCF, P-CSCF, I-CSCF, HSS), ktoré tvoria jadro Open IMS projektu pracujú na open source softvéri, ako je napr. SER (SIP Express Router), alebo MySQL [33].

SIP Express Router je výkonný, konfigurovateľný, voľne dostupný SIP server, šírený pomocou open source GPL (General Public License) licencie. Môže pracovať ako SIP prihlasovací server, proxy server, alebo preposielací server. SER podporuje rôzne druhy databáz, ako sú napr. MySQL, PostgreSQL [32].

Open source IMS Core System poskytuje implementáciu IMS subsystému určenú na testovanie IMS aplikácií, ktorá taktiež slúži na výskumné účely. Hlavnými entitami Open Source IMS Core projektu sú Open IMS CSCF entity (Proxy, Interrogating a Serving), ktoré boli vyvinuté ako rozšírenie SER. Open IMS architektúru je možné rozšíriť aj o E-CSCF a LRF (Location Routing Function) entity. FOKUS poskytuje virtuálne CD, ktoré obsahuje virtualizovaný operačný systém Linux dostupný v dvoch distribúciach (Gentoo, Ubuntu), na ktorých je nasadená platforma Open IMS. CD možno zdarma stiahnuť na adrese [34]. Podmienky použitia sú taktiež uvedené na tejto adrese.

3.1.1 FHoSS

FOKUS vyvinul vlastný typ HSS databázy FHoSS (FOKUS Home Subscriber Server). Databáza FHoSS je postavená na technológii SER. Dáta užívateľov sú uložené v MySQL databáze. FHoSS poskytuje databázový riadiaci systém a konfigurátor pre rozhrania medzi CSCF prvkami. FHoSS umožňuje generovanie autentifikačných vektorov a poskytuje webové konfiguračné rozhranie pre jednoduchú správu užívateľských profilov a príslušných CSCF entít [11]. Architektúra Open IMS Core systému je zobrazená na obrázku 3.1.



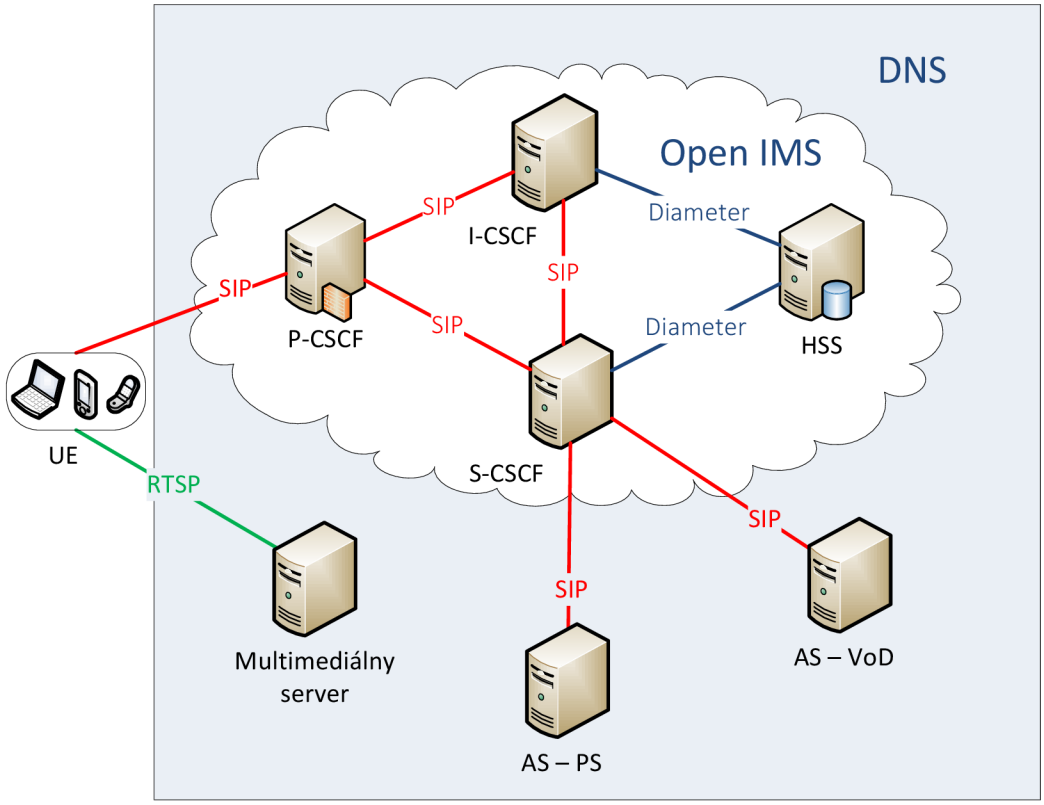
Obr. 3.1: Architektúra Open IMS Core systému [32].

Funkcie FoHSS:

- podpora Cx rozhrania,
- podpora Sh rozhrania,
- podpora Zh rozhrania,
- podpora AuC funkcionality,
- webové konfiguračné rozhranie.

3.1.2 Open IMS v školskej sieti

V školskej sieti na Fakulte elektrotechniky a komunikačních technologií (FEKT) v Brne je nasadený Open IMS projekt, ako súčasť experimentálnej IMS siete. Na obrázku 3.2 je znázornená architektúra tejto siete. Systém tvorí jadro s Open IMS core prvkami (P-CSCF, S-CSCF, I-CSCF a HSS). Komunikácia medzi jednotlivými prvkami je zaistená pomocou SIP a DIAMETER protokolov. V experimentálnej sieti sa tiež nachádza multimediálny server, ktorý komunikuje s účastníckym zariadením UE, prostredníctvom RTSP (Real-Time Streaming Protocol) protokolu. Aplikačné servery AS-PS prezenčný server (*angl. Presence Server*) a AS-VoD video na požiadanie (*angl. Video on Demand*) poskytujú služby užívateľom.



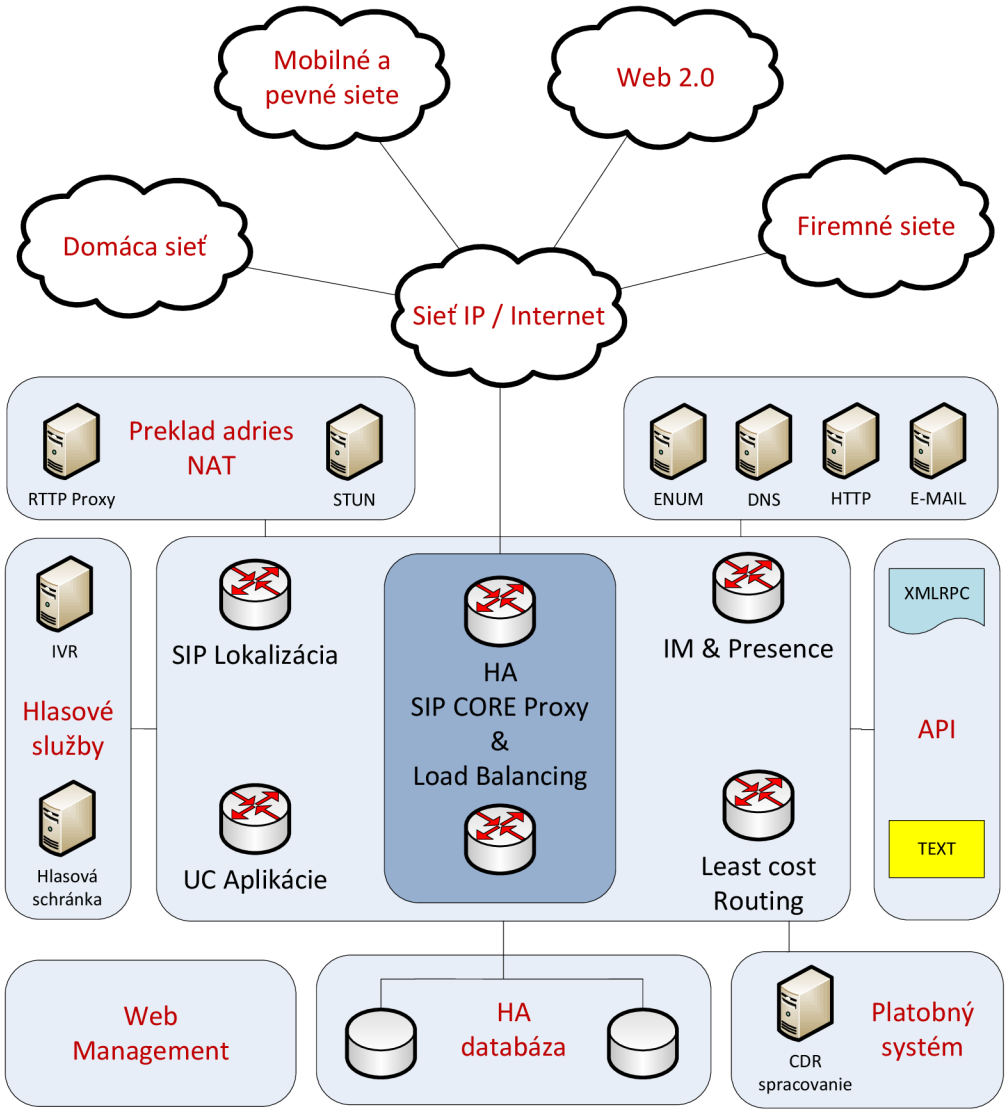
Obr. 3.2: Open IMS systém nasadený v školskej sieti.

3.2 Kamailio IMS

Projekt Kamailio IMS (bývalý OpenSER) je postavený na Kamailio SIP serveroch, ktoré sú vyvíjané pod open source licenciou GPL. Je schopný obslúžiť tisíce spojení za sekundu. Podporuje veľké množstvo funkcií, napr. TCP, UDP, SCTP, zabezpečenú VoIP komunikáciu prostredníctvom TLS protokolu. Podporuje IPv4 a IPv6 adresovanie, spoplatnenie, autentizáciu a autorizáciu. Kamailio IMS taktiež podporuje viaceré databázové systémy, ako sú MySQL, Postgres a Oracle. Medzi funkcie Kamailio SIP serveru patrí aj vzdialené volanie procedúr XML-RPC (Remote Procedure Call) a SNMP. XML-RPC dáta sú prenášané pomocou HTTP transportného protokolu a kódované pomocou XML (Extensible Markup Language) [16].

3.3 Little IMS

Little IMS projekt predstavuje open source implementáciu niekoľkých IMS/TISPAN sieťových prvkov. Cieľom Little IMS projektu je poskytnúť väčšinu možností, ktoré ponúka IMS sieť v jednoduchej a rozšíriteľnej podobe. Dokumentáciu k Little IMS projektu možno nájsť na [18].



Obr. 3.3: Komunikačná platforma Kamailio [17].

3.3.1 Komponenty Little IMS

Little IMS pozostáva z nasledujúcich častí. [18]

- S-CSCF, ktoré poskytuje:
  - Mw rozhranie
    - umožňuje IMS terminálom pripojenie k S-CSCF,
    - slúži na komunikáciu medzi CSCF entitami,
    - a ISC rozhranie, ktoré umožňuje integrovanie AS.
  - Mr rozhranie pre komunikáciu s MRFC.
  - Cx rozhranie pracujúce na protokole DIAMETER, slúžiace na komuni-

káciu s HSS.

- HSS databáza.
  - Cx rozhranie spája S-CSCF a I-CSCF, a pracuje na protokole DIAMETER.
  - Webové rozhranie.
- P-CSCF.
- I-CSCF.
  - Cx rozhranie na pripojenie k HSS.

3.4 IMS Zone

Projekt IMS Zone zahŕňa IMS core komponenty pod formálnym označením „Core Components for 4th Generation Telecomm Infrastructure“. Projekt predstavuje implementáciu 3GPP štandardu, ktorý definuje IMS core prvky, HSS, online platobný systém (*angl. Online Charging System*), offline platobný systém (*angl. Offline Charging System*), multimediálny server a OAM&P (Operation, Administration, Maintanance & Provisioning) systém [15]. Jednotlivé entity sú implementované vo modulárnom asynchrónnom vývojovom prostredí AMPS (Asynchronous Middleware for Protocol Servers). AMPS je open source vývojové prostredie založené na GPL licencii. Viac informácií o AMPS možno nájsť na [7].

3.5 Advanced IMS

Advances IMS Inc. poskytuje širokú ponuku AAA a NMS produktov pre IP siete vrátane IMS. Jednotlivé komponenty vychádzajú z 3GPP a 3GPP2 štandardov. Medzi ponúkané služby a produkty patria: Diameter AAA Server, IMS online a offline spoplatnenie, IMS HSS, NMS (Network Management System), Radius AAA a pokročilé sprostredkovanie (*angl. Advanced Mediation*). Sprostredkovanie je proces transformácie informácií o hovoroch CDR (Call Detail Records), alebo informácií o využitých službách UDR (Usages Details Records), z jedného formátu na iný formát. Príkladom môžu byť dáta generované jedným poskytovateľom služieb a ich následné spracovanie iným poskytovateľom. Viac informácií a dokumentáciu jednotlivých produktov možno nájsť na stránkach [6].

3.6 NGNLAB

NGNLAB projekt predstavuje spoluprácu Slovenskej technickej univerzity v Bratislave (STUBA) a súkromných spoločností na výskumnom projekte v oblasti NGN

sietí. NGN sieť založená na IMS platforme je postavená na open source technológii Open IMS, ktorá poskytuje flexibilitu a možnosti rozšírenia a modifikácie. Core prvky IMS siete v NGNLAB pracujú na serveroch, na ktorých je nasadený operačný systém Linux v distribúcii Debian. Multimediálne služby (video, hlas, web), ako sú posielanie správ, video na požiadanie VoD, webové služby a iné sú zabezpečené pomocou technológií: Mobicents, Freeswitch, Asterisk, OpenSIPS, XMPP (Extensible Messaging and Presence Protocol) servera a ďalších. Kompletný zoznam možno nájsť na adrese [23].

NGNLAB poskytuje zdarma na testovanie live CD s Open IMS Core technológiou. Pôvodnú verziu Open IMS Core platformy možno nájsť na [34]. NGNLAB ponúka upravenú verziu tohto open source systému, kde bolo vyvinuté nové konfiguračné webové rozhranie v ktorom možno štartovať, zastavovať a reštartovať bežiace IMS služby s možnosťou zmeny IP adries core prvkov. Takisto bola vytvorená možnosť upravovať konfiguračné súbory I-CSCF, S-CSCF, P-CSCF entít prostredníctvom webového rozhrania. Live CD možno stiahnuť na adrese [24], kde je uvedený odkaz na stiahnutie.

4 POŽIADAVKY A NÁVRH DOHĽADOVÉHO SYSTÉMU

4.1 Požiadavky pre dohľadový systém

Na začiatku návrhu a tvorby dohľadového systému bolo vytýčených niekoľko základných požiadaviek, ktoré by mal výsledný dohľadový systém spĺňať. Ako prvé bolo potrebné zaistiť komunikáciu medzi serverom, na ktorom bude bežať funkčný dohľadový systém a jednotlivými prvkami Open IMS siete. Dohľadový systém bude musieť zbierať potrebné informácie o stave jednotlivých Open IMS prvkov, ktoré predstavujú samotné počítače. Cieľom dohľadového systému bude teda vzdialená kontrola stavu jednotlivých core prvkov Open IMS site (P-CSCF, S-CSCF, I-CSCF a HSS) z pohľadu vyťaženia pamäte, procesora a disku každého systému. Výsledok by mal byť graficky spracovaný v prehľadných grafoch.

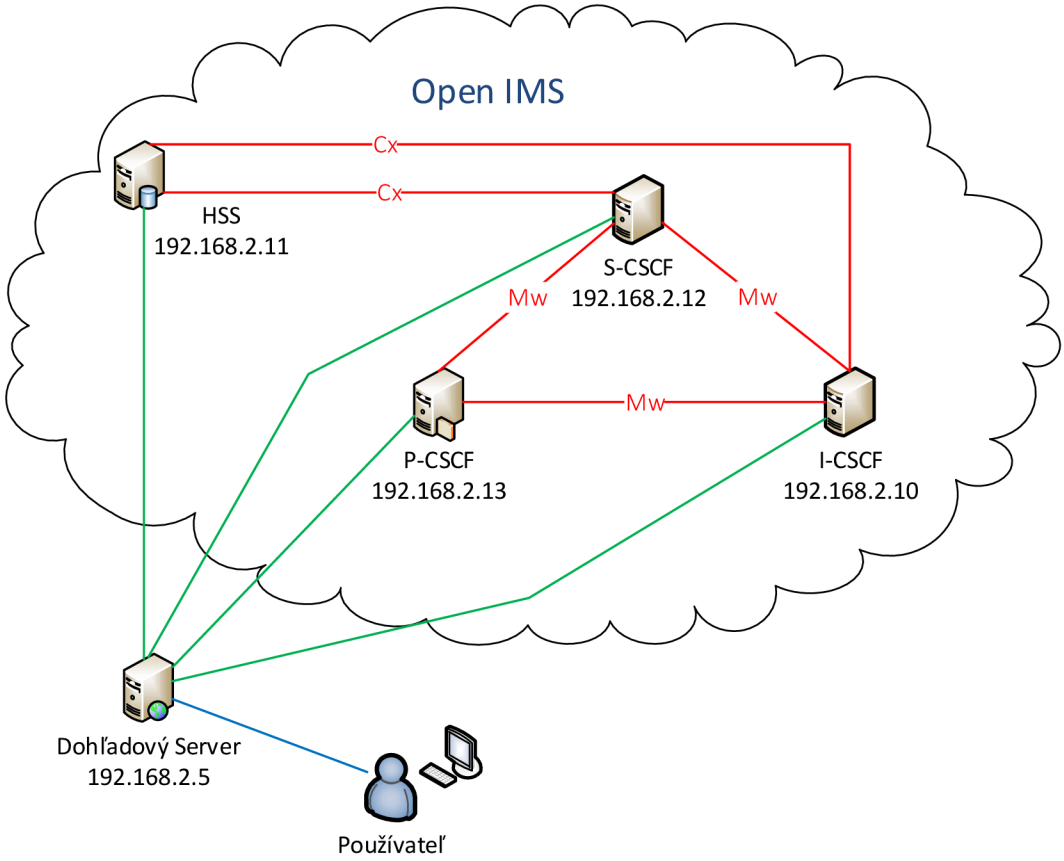
Pre získavanie všetkých potrebných dát určených pre monitoring serverov bude potrebné na každý sever nasadiť agenta, ktorý bude tieto údaje v pravidelných intervaloch zbierať a posielať na dohľadový server, na ktorom bude nainštalovaná serverová aplikácia určená pre monitoring. Bude potrebné navrhnúť a nakonfigurovať samostatný server, z ktorého budu monitorované jednotlivé core prvky Open IMS siete. Užívateľ bude prostredníctvom webového rozhrania aplikácie, ktorá bude umiestená na dohľadovom serveri, vzdialene pristupovať k jednotlivým prvkom Open IMS systému.Grafické znázornenie architektúry dohľadového systému je uvedené na obrázku 4.1.

Ďalšou požiadavkou je vzdialený prístup k jednotlivým súborom Open IMS siete, ktoré sa nachádzajú v adresári `/opt/OpenIMSCore` na jednotlivých core prvkoch. Cieľom bolo zaistiť okrem prístupu, k týmto súborom aj možnú editáciu každého súboru, ktorý sa nachádza v stromovej štruktúre adresára `/opt/OpenIMSCore`, kde sú inštalované jednotlivé skripty a súbory Open IMS siete, podľa typu toho ktorého core prvku.

Jednou z požiadaviek bolo umožniť užívateľovi základný prehľad o prebiehajúcej komunikácii na linkách medzi jednotlivými core prvkami Open IMS siete. Komunikáciu na linkách (traffic) bolo potrebné odchytávať na každom core prvku a následne zaistiť jednoduchú analýzu zachytených dát. Spolu s analýzou dát, boli všetky údaje spracované do prehľadných grafov, využitím open source nástrojov popísaných v nasledujúcej kapitole.

4.2 Architektúra

Na obrázku 4.1 je zobrazená navrhnutá architektúra dohľadového systému z pohľadu prepojenia jednotlivých core prvkov Open IMS siete. Rozhrania medzi jednotlivými core prvkami (P-CSCF, S-CSCF, I-CSCF a HSS) sú prepojené prostredníctvom liniek Mw a Cx. Ich bližší popis možno nájsť v kapitole 1.6. Z jednotlivých core prvkov vedie spojenie k dohľadovému serveru, ktorý je nosným prvkom navrhnutej architektúry a pracuje na ňom dohľadový systém. Na obrázku je tiež znázornená IP konfigurácia siete.

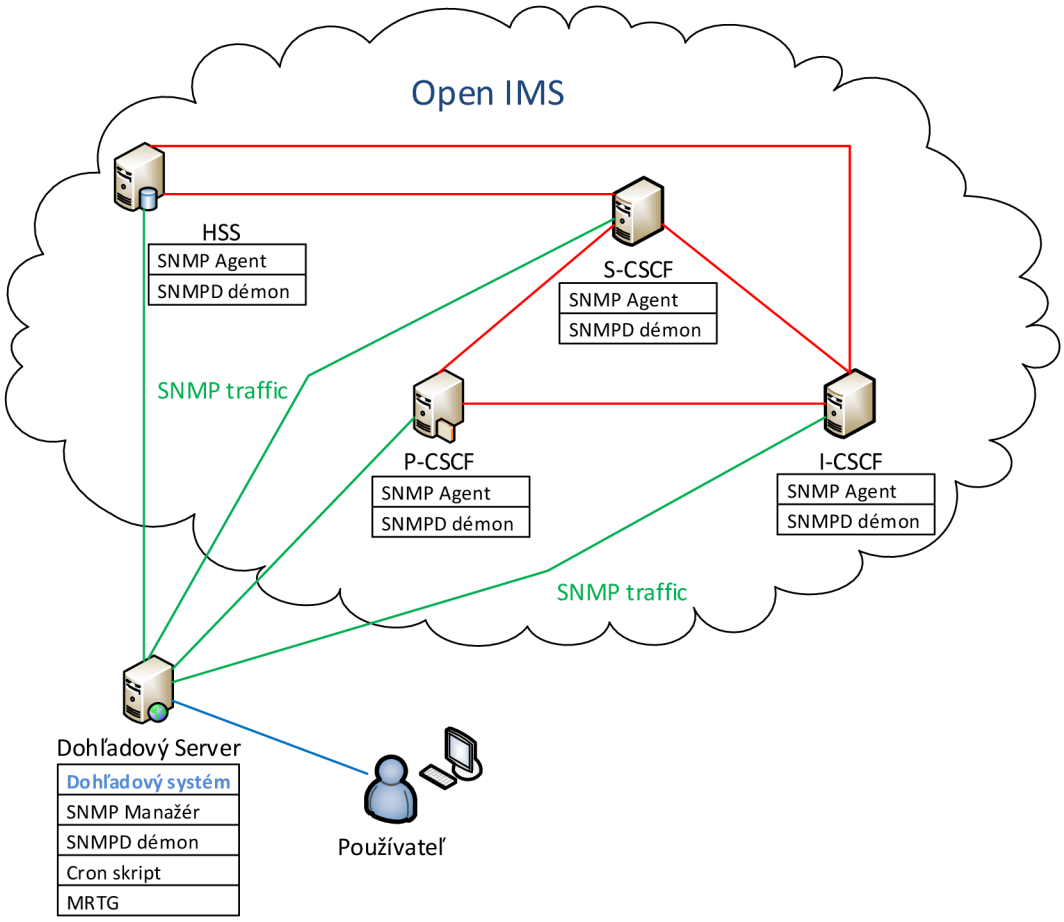


Obr. 4.1: Návrh architektúry dohľadového systému.

4.2.1 Architektúra z pohľadu SNMP

Keďže na zber informácií o stave jednotlivých core prvkov z pohľadu vyťaženia CPU, RAM a HDD bude využitý monitorovací systém MRTG (Multi Router Traffic Grapher), ktorý na komunikáciu s klientskými stanicami využíva SNMP protokol, bolo na jednotlivých klientov (v tomto prípade core prvky Open IMS siete) potrebné

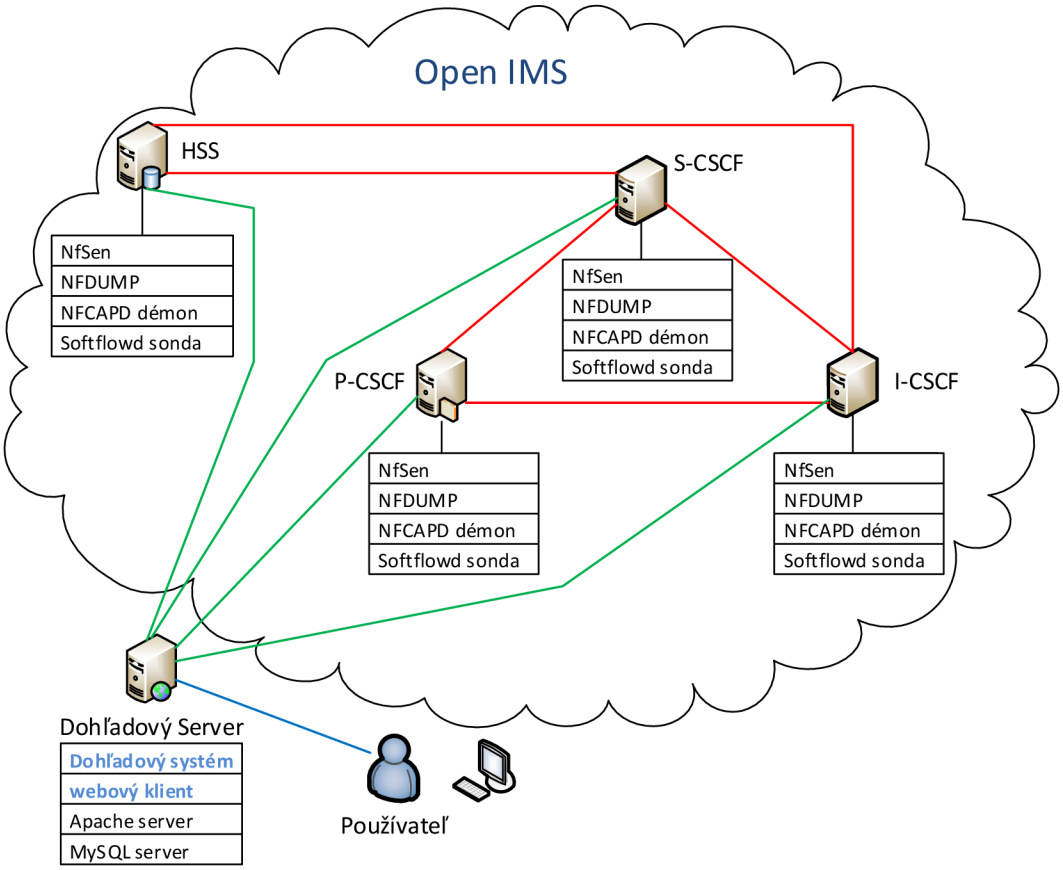
implementovať a nakonfigurovať SNMP agentov. Konfigurácia je bližšie popísaná v kapitole 6.3. Na obrázku 4.2 je následne zobrazená architektúra z pohľadu komunikácie a výmeny dát prostredníctvom SNMP protokolu, medzi dohľadovým serverom a core prvkami Open IMS siete.



Obr. 4.2: Architektúra z pohľadu SNMP komunikácie.

4.2.2 Architektúra dohľadového systému a komponentov

Obrázok 4.3 znázorňuje štruktúru dohľadového systému a uvádza jednotlivé komponenty, ktoré bolo potrebné nainštalovať a nakonfigurovať, aby bolo možné monitorovať sieťovú komunikáciu (*angl. traffic*) na core prvkoch open IMS siete. Obrázok zároveň zobrazuje dohľadový server, na ktorom je nakonfigurovaný samotný dohľadový systém v podobe webovej aplikácie. Konfigurácia a bližší popis implementácie monitorovacieho systému na zachytávanie NetFlow dát je popísaná v kapitole 6.4.

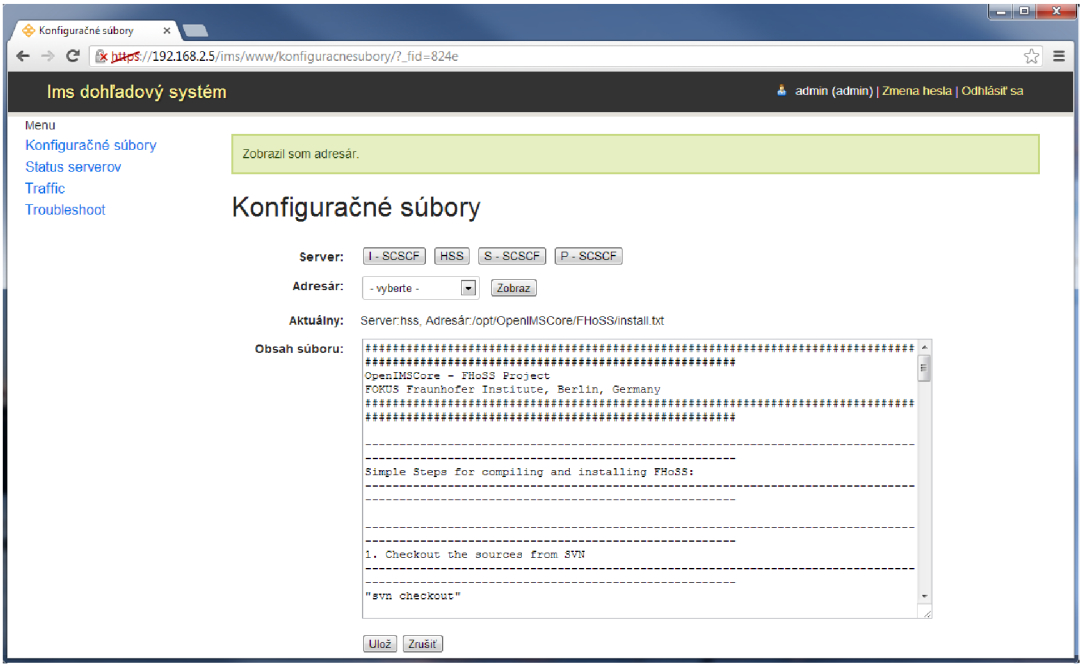


Obr. 4.3: Architektúra komponentov dohľadového systému.

4.3 Návrh webového dohľadového systému

Návrh aplikácie dohľadového systému je znázornený na obrázku 4.4. Jednoduché a prehľadné rozhranie sa skladá z menu, v ktorom sú uvedené jednotlivé položky, slúžiace na dohľad a prípadnú konfiguráciu entít Open IMS siete. Pred prvým vstupom do aplikácie je nutné zaregistrovať sa a vytvoriť si užívateľský účet vyplnením mena, emailovej adresy a hesla. V základe sú vytvorené dve užívateľské skupiny „admin“ a „user“. Práva jednotlivých užívateľských kont sú uvedené v kapitole 4.3.3.

K položke *Konfiguračné súbory* bude mať prístup len administrátor. Prístupové mená a heslá sú uvedené v prílohe A.1. Pri prihlásení z ostatných užívateľských účtov, nebude táto položka viditeľná v aplikácii. V tejto záložke bude môcť administrátor vzdialene pristupovať k jednotlivým konfiguračným súborom pomocou webového rozhrania. Administrátor má možnosť vybrať si z jednotlivých serverov P-CSCF, S-CSCF, I-CSCF, alebo HSS konkrétny súbor (konfiguračný skript, textový dokument, atď). Konfiguračné súbory jednotlivých serverov sú štandardne uložené v ad-



Obr. 4.4: Zobrazenie aplikácie IMS dohľadového systému.

resári `/opt/OpenIMSCore`. Administrátor bude mať možnosť tieto súbory prezerať a prípadne aj upravovať priamo vo webovom rozhraní aplikácie. Webové rozhranie konfiguračných súborov je zobrazené na obrázku 4.4.

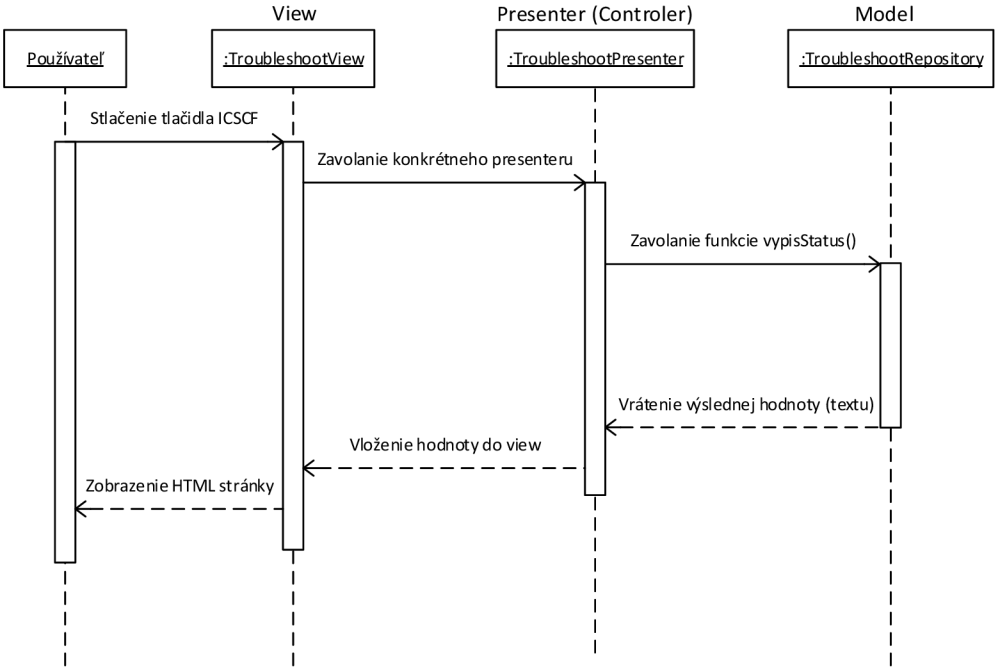
V sekcii *Status Serverov* bude možný monitoring jednotlivých serverov. Je možné kontrolovať vyťaženie CPU, RAM, a HDD každého servera. Dáta sú pravidelne zbierané zo serverov v 5 minútových pravidelných intervaloch. Ukážka vytvoreného grafu je uvedená na obrázku 6.2. Na jednotlivých klientoch je nainštalovaný SNMP agent, ktorý slúži na zber dát. Grafy sú vykresľované pomocou MRTG monitorovacieho nástroja. Bližšia konfigurácia je uvedená v kapitole 6.3.2.

Záložka *Traffic* bude slúžiť na monitorovanie komunikácie na linkách medzi servermi. Bude monitorovaný traffic na rozhraní Mw, ktoré prepája P-CSCF, S-CSCF a I-CSCF, a na rozhraní Cx, ktoré spája HSS s S-CSCF a I-CSCF. K monitoringu bude potrebné zaistiť základnú analýzu NetFlow dát. Podstránka Traffic je tvorená pomocou monitorovacieho nástroja NfSen, ktorý monitoruje sieťovú komunikáciu na linkách jednotlivých serverov. Popis činnosti a monitoringu je uvedený v kapitole 6.4.

Posledná položka v menu s názvom *Troubleshoot* obsahuje viaceré príkazy, ktorými možno skontrolovať napríklad bežiace procesy, čas behu servera (*angl. uptime*), využitie pamäte a ďalšie.

4.3.1 Návrhový vzor MVC

Model MVC (Model-View-Controller) bol zvolený pri vývoji webovej časti dohľadového systému z dôvodu rozčlenenia a logického oddelenia jednotlivých prvkov aplikácie. MVC zjednodušene predstavuje rozdelenie aplikácie do troch vrstiev. Prvá vrstva je Model, ktorá predstavuje aplikačnú logiku a zaisťuje základnú činnosť aplikácie. Akcie užívateľa (prihlásenie, výber položky v menu), predstavujú vykonané akcie pomocou modelu. Vrstva View predstavuje užívateľské rozhranie webovej aplikácie. Táto vrstva je zodpovedná za získavanie dát od užívateľa a zobrazovanie výslednej aplikácie, v tomto prípade dohľadového systému. Vrstva Controller je umiestená medzi vrstvami Model a View. Spracováva požiadavky užívateľa a na ich základe potom volá vhodný Model. Na obrázku 4.5 je zobrazené použitie MVC v IMS dohľadovom systéme v sekcii Troubleshoot [21].



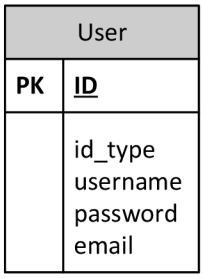
Obr. 4.5: Sekvenčný diagram pre Troubleshoot.

Princíp modelu MVC je názorne ukázaný na sekvenčnom diagrame pre podstránku Troubleshoot. Po otvorení stránky sa pre používateľa zobrazí konkrétny pohľad (*angl. view*), v ktorom sa nachádza formulár. Po stlačení odosielacieho tlačidla ICSCF, sa zavolá súbor `TroubleshootPresenter`, v ktorom je zadefinované príkazy, ktoré sa majú vykonať. Následne sa zavolá funkcia `vypisStatus()`, ktorej kód

sa nachádza v modeli, čiže v súbore `TroubleshootRepository`. Táto funkcia sa vykoná a vráti konkrétnu hodnotu, čiže v našom prípade textový výpis príkazu, ktorý sme si zvolili. O túto hodnotu sa znova postará presenter (controller), ktorý ju vloží do view a samotný view potom znova vykreslí textový výpis zvoleného príkazu pre užívateľa.

4.3.2 Návrh databáze

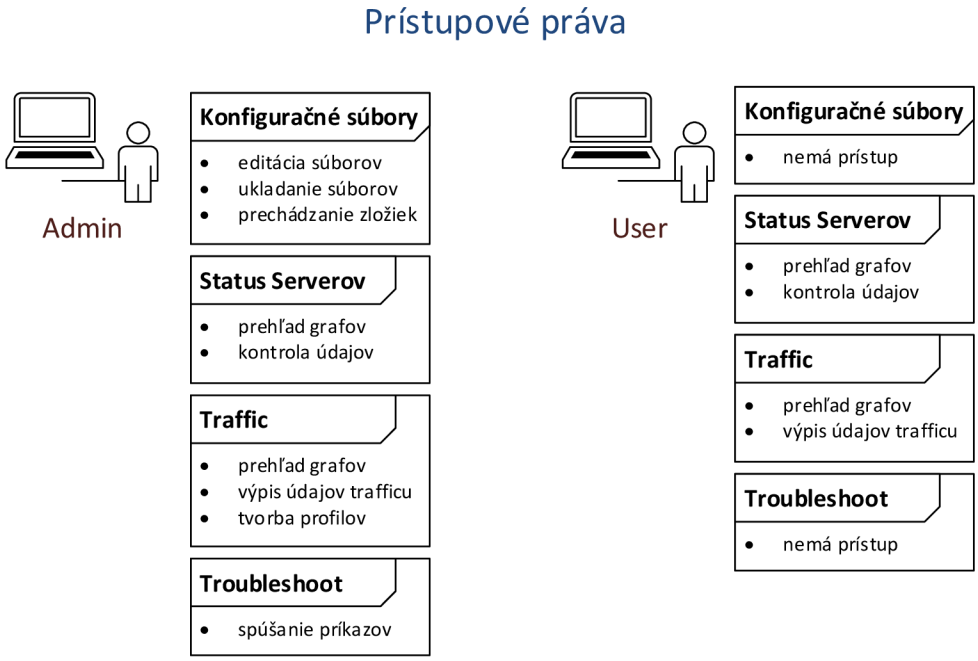
Navrhnutá databáza obsahuje jednu tabuľku **User** 4.6, ktorá má nastavené nasledovné atribúty: id, id_type, username, password a email. ID slúži ako primárny kľúč relácie, obsahuje unikátnu hodnotu, ktorá jednoznačne identifikuje každý záznam tabuľky. Parameter id_type môže nadobúdať dve hodnoty „0“ a „1“ , pričom v aplikácií sú týmto dvom hodnotám pridelené nasledovné role: označenie „0“ je pridelené administrátorovi, ktorý má nastavené administrátorské práva a označenie patrí „1“ bežnému užívateľovi. Položka „username“ obsahuje meno, ktoré si používateľ zvolil pri registrácii. V položke „password“ sa nachádza používateľovo heslo, vo forme hash kódu. Posledná položka „email“ obsahuje emailovú adresu používateľa. Emailová adresa mala byť pôvodne určená pre posielanie emailového overenia. Táto funkcia však nie je implementované v aktuálnej verzii dohľadového systému, ale možno ju využiť do budúcnosti.



Obr. 4.6: Tabuľka databázy.

4.3.3 Možnosti spravovania dohľadového systému

Pre správu dohľadového systému Open IMS siete boli navrhnuté dva typy užívateľských kont. Podľa stupňa oprávnení môžu byť užívatelia dohľadového systému priradení do kategórie User alebo Admin. Každá skupina má pridelené iné práva a možnosti meniť, upravovať, prípadne prezerať jednotlivé parametre Open IMS siete a príslušných serverov.



Obr. 4.7: Prístupové práva

User

Požívateľský účet „user“ je určený pre užívateľov oboznámených s základnou štruktúrou Open IMS systému. Používateľ typu user má prístup k informáciám o stave serverov a môže si ich prezerať a kontrolovať ich stav. V položke Traffic má možnosť prezerať si výsledné grafy získané z NetFlow dát a takisto si môže zobraziť ľubovolné dostupné štatistiky. Nemá však oprávnenie k vytváraniu nových profilov. User prístup ku konfiguračným súborom a nemá oprávnenia používať príkazy v záložke Troubleshoot.

Admin

Administrátor prihlásený pod užívateľským kontom „admin“ má plnú kontrolu nad správou všetkých serverov. Administrátor prístup ku kompletnej správe serverov P-CSCF, S-CSCF, I-CSCF a HSS. Môže pristupovať ku všetkým konfiguračným súborom na jednotlivých serveroch. Má právo editácie konfiguračných súborov, ukladania jednotlivých zmien a prechádzanie zložiek. Konfiguračné súbory sú uložené v adresári `/opt/OpenIMSCore` na všetkých serveroch. Z dôvodu bezpečnosti je adresár `/opt/OpenIMSCore` nastavený ako hlavý a nemožno pristupovať o úroveň vyššie. Prístup k týmto konfiguračným súborom bude zaistený pomocou jednoduchého rozhrania vo webovom rozhraní dohľadového systému. V položke Status Serverov má

admin nastavené rovnaké práva ako user. V nemu Traffic má nastavené takisto rovnaké práva ako user naviac doplnené o možnosť vytvárať nové profily pre zachytávanie sieťovej komunikácie na linkách. Administrátor môže využívať všetky dostupné príkazy v položke Troubleshoot, teda posielať ICMP request (ping) na server, kontrolovať čas behu servera (*angl. uptime*) jednotlivých core prvkov a podobne. Všetky dostupné príkazy sú uvedené na obrázku 4.8. Nastavené prihlasovacie mená a heslá sú uvedené v prílohe A.1.

Obr. 4.8: Dostupné príkazy v sekcii Troubleshoot.

5 TVORBA DOHĽADOVÉHO SYSTÉMU

V nasledujúcej kapitole budú stručne popísané jednotlivé zvolené technológie, ktoré boli použité pri tvorbe jednoduchého dohľadového systému pre experimentálnu sieť Open IMS. Použité technologické riešenia sú voľne dostupné (open source), založené na GPL licencii.

5.1 Použité technológie

5.1.1 PHP

Pre vývoj dohľadového systému vo webovom rozhraní bol primárne použitý skriptovací jazyk PHP, aktuálne dostupný vo verzii PHP 5.3.23. (máj 2013) [35]. Dôvodom použitia PHP jazyka sú jeho bohaté možnosti v oblasti vývoja webových aplikácií a jeho široká možnosť nasadenia. To, čím sa odlišuje PHP napríklad od JavaScript-u, je to, že JavaScript pracuje na strane klienta, zatiaľ čo PHP skripty sú spracované na serveri a na klientskú stranu posielajú spracovaný výsledok skriptu. PHP sa veľmi často používa pri tvorbe a vývoji dynamického webu. Podporuje spoluprácu s veľkým množstvom protokolov ako sú napr. LDAP (Lightweight Directory Access Protocol), SNMP, IMAP (Internet Message Access Protocol), POP3 (Post Office Protocol) a mnohé ďalšie. Medzi iné dostupné riešenia v oblasti tvorby dynamického webu patria skriptovacie jazyky ASP (Active Server Pages) od spoločnosti Microsoft, CFML (ColdFusion Markup Language), JSP (JavaServer Pages) od spoločnosti Sun Microsystems (teraz Oracle) a ďalšie [35].

5.1.2 MySQL

Ako relačný databázový manažment systém RDBMS (*angl. relational database management system*) bol nasadený MySQL databázový systém, aktuálne dostupný v stabilnej verzii MySQL 5.0.8 (máj 2013). MySQL patrí medzi najpoužívanejšie relačné databázové systémy. Je obľúbený z dôvodu jednoduchosti nasadenia a je dostupný zdarma pod GNU General Public License (GPL) licenciou. Existuje veľké množstvo RDMBS systémov dostupných zdarma i v platenej verzii, (napr. Microsoft SQL Server, PostgreSQL, SQLite a iné). MySQL databázový systém na zhromažďovanie dát bol zvolený z dôvodu autorovej predchádzajúcej skúsenosti s týmto relačným systémom [22].

5.1.3 Apache

Výsledná webová aplikácia je spustená na webovom serveri Apache, ktorý je dostupný vo verzii 2.2.16 pre Debian. Webový server Apache bol zvolený z dôvodu jednoduchosti nasadenia, predchádzajúcej skúsenosti autora s prácou s Apache webovým serverom, jednoduchej správy systému a taktiež z dôvodu open source dostupnosti. Apache patrí k najrozšírenejšie nasadzovanému webovému systému v oblasti webových serverov na internete. Ďalšími alternatívami pre webový server sú systém IIS (Internet Information Services) od Microsoftu, nginx od spoločnosti NGINX, GWS (Google Web Server) od Google, Lighttpd a ďalšie [8], [25].

5.1.4 Ubuntu a Debian

Systém Open IMS nasadený v školskej sieti pracuje na operačnom systéme Linux v distribúcii Ubuntu, konkrétne Ububtu 12.04.1 LTS, kde označenie LTS (*angl. Long Term Support*) označuje verziu s dlhodobou podporov v rámci aktualizácií. Od vydania verzie 12.04 je podpora rovnako pre serverovú verziu i desktopovú verziu zhodne 5 rokov [51]. Pre jednoduchšiu prácu pri vývoji dohľadového prostredia, boli jednotlivé core prvky (P-CSCF, S-CSCF, I-CSCF a HSS) virtualizované, pričom každý z nich pracuje na operačnom systéme Linux v spomínanej distribúcii.

Pri výbere operačného systému, na ktorom bude pracovať dohľadový server, bolo dôležité zachovať kompatibilitu pri komunikácii s jednotlivými core prvkami Open IMS siete. Ako operačný systém, hosťujúci dohľadový systém bol zvolený Debian, konkrétne verzia 6.0.6. Aktuálne je dostupná stabilná (*angl. stable*) verzia Debianu s označením 7.0, vydaná 4. 5. 2013. Debian využíva ako jadro Linux, alebo FreeBSD. FreeBSD predstavuje operačný systém zahŕňajúci aj ďalší software. Systém Ubuntu, na ktorom je virtualizovaná Open IMS sieť, bol vyvinutý na základoch systému Debian, a z toho dôvodu sú vzájomne kompatibilné. Debian podporuje veľké množstvo počítačových architektúr ako sú napr. **amd64** pre 64 bitové procesory AMD a Intel, **i386** pre 32 bitové architektúry procesorov, **ia64** pre Intel Itanium a mnohé iné [9].

5.1.5 Nette

Ako programovací jazyk bol použitý skriptovací jazyk PHP 5.1.1. Z dôvodu rýchlejšej práce s PHP, eliminácie bezpečnostných rizík a dostupnosti ladiacich nástrojov pre odhalenie chýb, bol počas vývoja dohľadového systému využitý framework Nette v aktuálne dostupnej verzii 2.0.10. Framework predstavuje univerzálnu softvérovú platformu, ktorú je možné niekoľkokrát opakovane použiť na vývoj aplikácií. Nette obsahuje podporu technológií ako sú napr. AJAX/AJAJ (Asynchronous JavaScript

and XML/Asynchronous JavaScript and JSON), SEO (Search engine optimization), MVC (Model-view-controller) a iných. Iné možnosti použitia frameworku predstavujú riešenia ako Joomla, CakePHP, Yii framework a ďalšie [27].

5.2 Monitorovacie nástroje

Dôležitým požiadavkom pri vývoji dohľadového systému bola možnosť vykresľovať grafy zaťaženia CPU, systémovej pamäte RAM a pevného disku každého core prvku. Hlavným problémom tohto zadania bolo zistiť, akým spôsobom možno získavať požadované údaje zo vzdialených strojov a ich následné spracovanie a zobrazenie výsledkov v grafickej podobe vo webovom rozhraní dohľadového systému. Našťastie však existuje niekoľko open source systémových monitorovacích nástrojov, ktoré dokážu výsledky monitoringu priamo spracovať a zobraziť vo webovom rozhraní. Medzi tieto nástroje patrí najmä Nagios, Zabbix, Cacti, MRTG (Multi Router Traffic Grapher), NfSen a ďalšie. Práve posledné dva spomenuté nástroje (MRTG a NfSen) boli využité pri tvorbe dohľadového systému. V nasledujúcej časti práce sú uvedené dôvody výberu týchto nástrojov.

5.2.1 MRTG (Multi Router Traffic Grapher)

MRTG je open source monitorovací nástroj, ktorý zbiera a spracováva dáta z lokálnej, alebo vzdialenej stanice pomocou SNMP protokolu. Z pohľadu komplexnosti a zložitosti v porovnaní s nástrojmi ako sú Nagios, Zabbix a Cacti je MRTG jednoduchý monitorovací nástroj vhodný pre menšie projekty. Práve z tohto dôvodu bol využitý práve MRTG monitorovací nástroj na monitorovanie stavu jednotlivých core prvkov Open IMS siete.

MRTG nástroj vytvoril Tobias Oetiker a zdrojový kód je napísaný v jazyku Perl. Podporuje spoluprácu s SNMP a SNMPv2c (Simple Network Management Protocol Version 2). Výsledné grafy sú generované vo formáte PNG (Portable Network Graphics). Výhodou MRTG je tiež konštantná veľkosť log súborov, ktoré nemenia svoju veľkosť [31].

5.2.2 NfSen (Netflow Sensor)

NfSen prestavuje monitorovací nástroj, ktorý obsahuje *NetFlow* kolektor a analyzátor. *NetFlow* je sieťový protokol pre zber sieťovej komunikácie. NfSen je podobne ako MRTG dostupný pod open source licenciou. Na rozdiel od MRTG, NfSen slúži primárne k analýze a zberu dát o využití sieťových prostriedkov a ich následné

spracovanie a zobrazenie v grafickej podobe. NfSen predstavuje samotný webový frontend, ktorý zobrazuje výsledné grafy sieťovej prevádzky. Samotné monitorovanie prevádzky je uskutočňované pomocou *Softflowd* sondy, ktorá monitoruje sieťovú prevádzku na zvolených sieťových rozhraniach pomocou protokolu *NetFlow*. Možnosti nástroja NfSen: [29]

- Grafické zobrazenie sieťovej prevádzky: toky, pakety a bajty pomocou RRD (Round Robin Database).
- Spracovanie NetFlow dát v rámci určitého časového úseku.
- Vytváranie histórie a vlastných profilov.
- Možnosť pridať vlastné upozornenia na základe určitých podmienok.
- Možnosť rozšírenia pomocou pluginov.

6 INŠTALÁCIA A KONFIGURÁCIA PRVKOV DOHĽADOVÉHO SYSTÉMU

6.1 Pripojenie dohľadového servera

Pri tvorbe dohľadového systému bolo potrebné vyriešiť spôsob komunikácie dohľadového systému, ktorý bude bežať vo webovom rozhraní s jednotlivými core prvkami. Samotné pripojenie je realizované pomocou SSH (Secure Shell). Nasledujúca ukážka zobrazuje časť kódu, ktorý sa využíva na pripojenie dohľadového servera k I-CSCF core prvku:

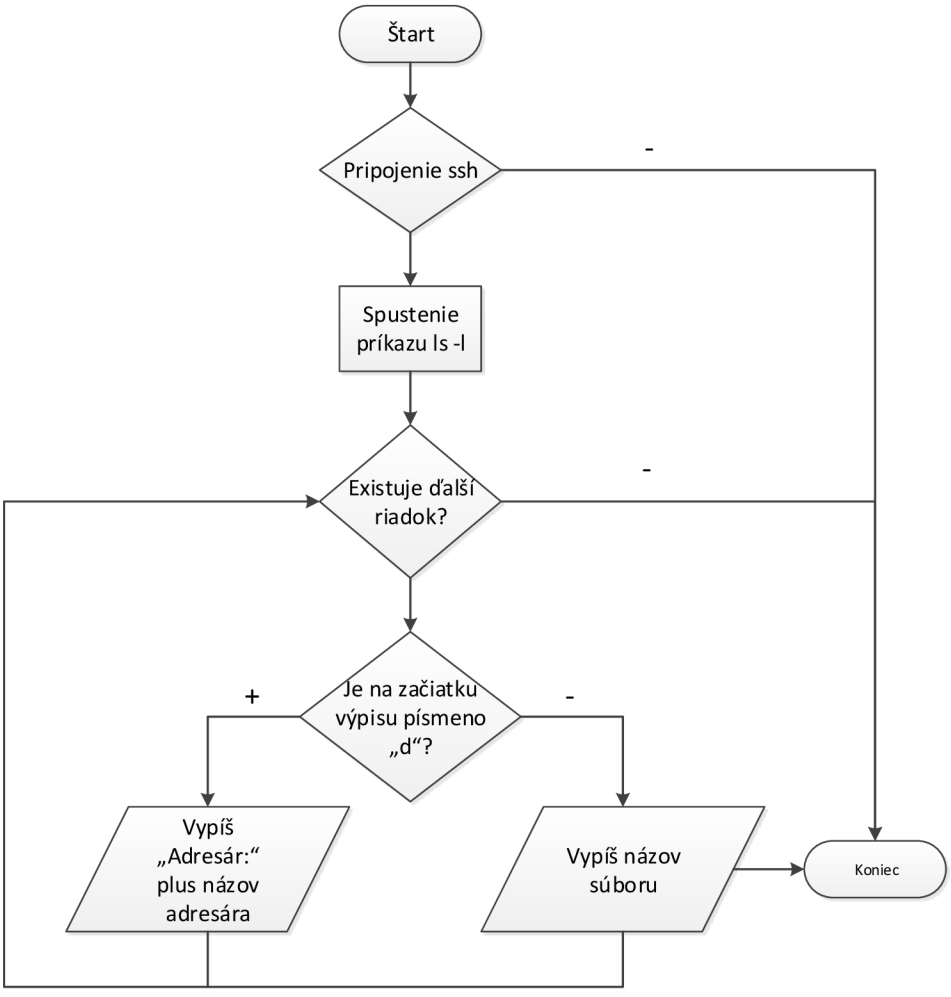
```
function pripojSsh($server) {
    if ($server=='icscf') {
        $host=gethostbyname('icscf');
        $user = "ims";
        $password = "ims1net2";
        }
    $ssh = @ssh2_connect($host);
    try{
        if (!$ssh) {
        throw new Exception("Nemozem sa pripojit na server");
        }
    $sshLogin = ssh2_auth_password($ssh, $user, $password);
    if (!$sshLogin) {
        die("Chyba - Nemozem sa prihlasit na server.\n");
    }
    return $ssh;
```

Funkcia na pripojenie dohľadového servera ku core prvkom funguje nasledovne. Najskôr sa podľa názvu serveru nastavia parametre daného serveru do premenných, čiže jeho IP adresa, meno servera (core prvku) a heslo. V ukážkovom prípade je to server „icscf“. Do premennej `host` sa pomocou funkcie `gethostbyname` zistí IP adresa I-CSCF core prvku, ktorá je uvedená v súbore `/etc/hosts` na dohľadovom serveri. V premenných `user` a `password` je uložené prihlasovacie meno a heslo potrebné na pripojenie dohľadového servera ku core prvku I-CSCF.

V druhom kroku sa pomocou funkcie `ssh2_connect` pokúsime pripojiť na vzdialený SSH sever. Ak je pripojenie úspešné, pokračujeme ďalej. Ak pripojenie zlyhá, nastane výnimka a vypíše sa chybová hláška „Nemôžem sa pripojiť na server“. V treťom kroku sa pokúsime autentizovať s použitím funkcie `ssh2_auth_password` a dohľadový systém sa pokúsi pripojiť ku konkrétnemu core prvku pomocou prihlasovacích údajov zadaných v prvej časti skriptu. Ak autentizácia prebehne úspešne, vráti sa ako parameter SSH spojenie a dohľadový server sa pripojí k core prvku I-CSCF. V prípade zlyhania autentizácie sa vypíše chybová hláška s názvom serveru na ktorý zlyhala autentizácia.

6.2 Konfiguračné súbory

Na obrázku 6.1 je znázornený vývojový diagram pre určovanie typu súboru, ktorý sa zobrazuje v rolovacom menu v sekcii konfiguračné súbory. Keďže pri prechádzaní stromovou štruktúrou bolo potrebje jasne definovať, ktorý súbor je typu adresár a ktorý súbor možno vypísať na editovanie v dohľadovom systéme. Rozhodovací algoritmus funguje tak, že najskôr sa vytvorí spojenie ssh s konkrétnym serverom. Vzdialene sa odošle príkaz `ls -l`, ktorý vypíše stromovú štruktúru adresárov a súborov. V linuxe je adresár označený písmenom „d“ a podľa toho sa algoritmus rozhoduje, či bude v rolovacom menu zobrazený ako adresár, alebo ako obyčajný súbor.



Obr. 6.1: Vývojový diagram pre zisťovanie adresára.

Podstránka konfiguračné súbory umožňuje pristupovať administrátorovi k konkrétnym konfiguračným súborom na jednotlivých core prvkoch Open IMS siete. Pre

ukladanie a zápis súborov bola vytvorená funkcia `ulozSubor`, ktorá funguje nasledovne. Najskôr sa vytvorí pripojenie ssh pomocou funkcie `pripojSsh`, ktorá je popísaná v kapitole 6.1. Nasledovne sa na tomto spojení vytvorí ešte pripojenie na sftp, pomocou funkcie `ssh2_sftp`, ktoré bude slúžiť na zabezpečený prenos súboru. Ďalej si načítame konkrétny súbor s parametrom pre zapisovanie do premennej `sftpStream`.

V ďalšom kroku si obsah konkrétneho súboru vložíme do pomocnej premennej, a takto pozmenený súbor pomocou funkcie `fwrite` uložíme. V priebehu tohto procesu postupne testujeme, či všetko prebehlo v poriadku a v prípade, že nastala chyba vyhodíme výnimku a vypíšeme zodpovedajúcu chybovú hlášku. V prípade že všetko prebehlo v poriadku uzatvoríme spojenie na sftp.

6.3 Inštalácia a konfigurácia MRTG a SNMP

6.3.1 Konfigurácia SNMP

Dôležitým prvkom na získavanie potrebných monitorovacích údajov pre MRTG je správna konfigurácia SNMP protokolu na dohľadovom serveri, ako aj na monitorovaných core prvkoch (P-CSCF, S-CSCF, I-CSCF a HSS). V prvom kroku, bolo potrebné nainštalovať potrebné balíčky SNMP a SNMPD na každý core prvok, vrátane dohľadového servera. SNMPD je démon (agent), ktorý odpovedá na SNMP požiadavky. Na základe požiadaviek zbiera požadované informácie na danom prvku a odosiela späť odpovede na požiadavky.

V druhom kroku prebiehala samotná konfigurácia SNMPD agentov na core prvkoch tak, aby dokázali komunikovať s dohľadovým serverom. V základnom nastavení SNMPD agentov je možné získať údaje iba z lokálneho stroja a preto museli byť upravené pôvodné konfiguračné súbory. V hlavnom konfiguračnom súbore `snmpd.conf` v časti fungovania agenta (*angl. agent behaviour*) bola zmenená pôvodná hodnota `agentAddress udp:127.0.0.1:161`, ktorá umožňuje komunikovať agentovi iba lokálne, na hodnotu `agentAddress udp:161` zaisťujúcu komunikáciu z dohľadového servera. SNMPD agent komunikuje na UDP porte 161.

V sekcii kontroly prístupu bola pridaná hodnota `view all included .1 80`, ktorá umožňuje čítať všetky hodnoty MIB dát 2.3.1. Ďalej boli nastavené položky:

```
com2sec local     localhost           public
com2sec mynetwork 192.168.0.0/24      public
```

kde parameter `com2sec` označuje zabezpečenie pomocou „community“ reťazca, ktorý je podobný heslu. Parametre `local` a `mynetwork` označujú bezpečnostné meno. Ďa-

lšie položky `localhost` a `192.168.0.0/24` označujú siete, z ktorých možno pristupovať pomocou SNMP. Posledná hodnota `public` predstavuje práve community reťazec.

Dôležitým bodom je kontrola správne nastavených hodnôt v súbore `/etc/default/snmpd`. Hodnota `SNMPDRUN` musí byť nastavená na „yes“, aby bolo zaistené, že SNMPD démon pracuje. Posledným krokom bolo nutné skontrolovať správne nastavenie SNMP démona pomocou príkazov:

```
ps aux | grep snmp
snmpwalk -v 2c -c public localhost IP-MIB::ipAdEntIfIndex
snmpwalk -v 2c -c public 192.168.2.12 IP-MIB::ipAdEntIfIndex
```

Pomocou prvého príkazu overíme, či pracuje SNMP démon medzi spustenými procesmi. Pomocou príkazu `snmpwalk` si overíme správnu funkčnosť SNMP najskôr na lokálnom pc, na ktorom sme konfigurovali SNMP a druhým príkazom si zo vzdialeného pc overíme funkčnosť SNMP. Označenia jednotlivých parametrov sú rovnaké, ako už boli spomínané vyššie v sekcii konfigurácie. Parameter `IP-MIB::ipAdEntIfIndex` označuje MIB súbor, ktorý nám vráti IP adresu nakonfigurovaných rozhraní. Pri konfigurácii boli využité poznatky z nasledujúceho zdroja [14].

6.3.2 Konfigurácia MRTG

Po správnom nakonfigurovaní SNMP bolo potrebné implementovať monitorovací systém MRTG. Samotný monitorovací systém bol nainštalovaný na dohľadovom serveri. Pre vykresľovanie grafov je potrebné spolu s MRTG nainštalovať niekoľko knižníc. Ako prvá bola nainštalovaná knižnica **ZLIB**, ktorá je potrebná pre generovanie grafických formátov. Ďalšou knižnicou je **LIBPNG**, ktorá slúži na generovanie grafov v formáte png. Poslednou knižnicou je knižnica **GD**. Je dôležité knižnice inštalovať v určenom poradí, pretože na seba nadväzujú a pri kompilácii využívajú predchádzajúce knižnice. Nainštalované boli nasledujúce verzie knižníc: zlib-1.1.7.tar.gz, libpng-1.6.1.tar.gz a gd-2.0.33.tar.gz.

Pri samotnej inštalácii MRTG využijeme predkompilačnú konfiguráciu pomocou skôr nainštalovaných knižníc:

```
./configure --prefix=/usr/local/mrtg       \
            --with-gd=/usr/local/src/gd    \
            --with-z=/usr/local/src/zlib    \
            --with-png=/usr/local/src/libpng
```

Celý čas pracujeme v adresári `/usr/local/`. Nakoniec pomocou príkazov `make` a `make install` spustíme samotnú kompiláciu MRTG. Pri konfigurácii boli použité informácie z [12].

6.3.3 Tvorba konfiguračných súborov

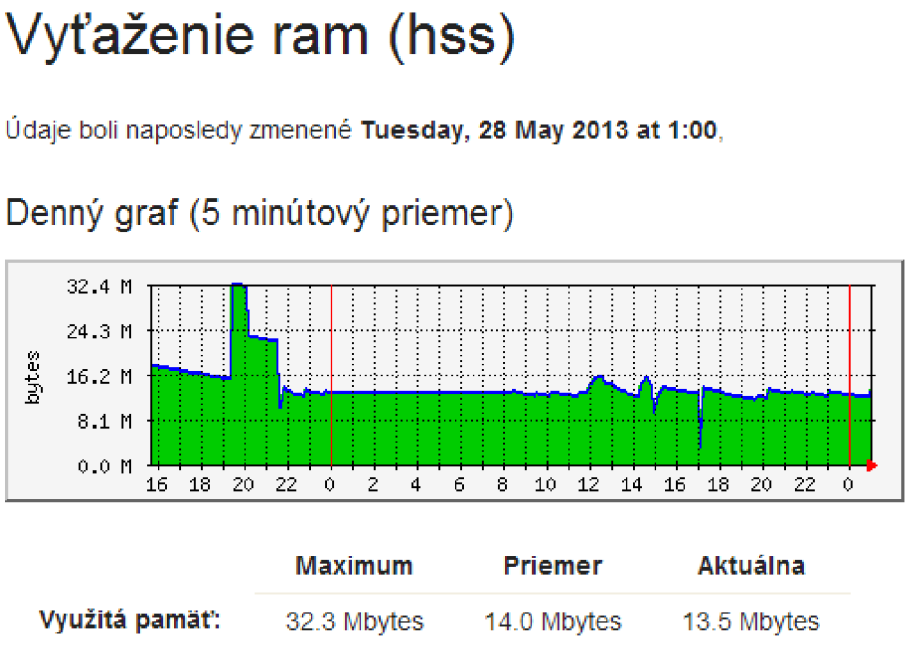
V základných požiadavkách v kapitole 4.1, boli uvedené tri parametre, ktorými sa bude monitorovať stav jednotlivých core prvkov a to stav CPU, RAM a HDD. Preto bude potrebné vytvoriť tri konfiguračné súbory pre každý core prvok, spolu teda dvanásť súborov. Ukážka konfiguračného súboru `cpu_icscf.cfg`, ktorý slúži na získavanie údajov o vyťažení CPU na I-CSCF core prvku je uvedená v prílohe B.1 spolu s ukážkami `disk_icscf.cfg` skriptu pre konfiguráciu disku a `ram_hss.cfg` pre konfiguráciu RAM.

```
WorkDir: /var/www/ims/www/mrtg/icscf/
Refresh: 300
LoadMIBs: /usr/local/share/snmp/mibs/UCD-SNMP-MIB.txt
Target[cpu_icscf]:ssCpuRawUser.0&ssCpuRawUser.0:public@icscf+
                  ssCpuRawSystem.0&ssCpuRawSystem.0:public@icscf+
                  sRawNice.0&ssCpuRawNice.0:public@icscf
RouterUptime[cpu_icscf]: public@icscf
```

Do adresára `WorkDir` sa ukladá výstup konfiguračného súboru. Refresh obnoví html stránku po 300 sekundách (5 minút), v ktorej sa vykreslí graf s novými získanými hodnotami. Parameter `LoadMIBs` určuje cestu k MIB súborom, konkrétne k `UCD-SNMP-MIB.txt` v ktorom sú popísané jednotlivé parametre použité v `Target [cpu_icscf]`. V položke Target je uvedená adresa `public@icscf` na ktorú sa dohľadový server pripája a zisťuje potrebné dáta. Na pripojenie používa community reťazec „public“ a názov hostname „icscf“, ktorého IP adresa je uložená v súbore `/etc/hosts`. Na podobnom princípe fungujú všetky ostatné konfiguračné súbory i pre RAM a HDD, s tým rozdielom, že sa využíva iný MIB súbor. Všetky konfiguračné MRTG súbory sú uložené na dohľadovom serveri v adresári `/usr/local/mrtg/cfg/`. Ukážkové konfiguračné súbory možno nájsť na [26] a [20].

```
0-59/5 * * * * root     LANG=C /usr/local/mrtg/bin/mrtg /usr/local/mrtg/cfg/cpu_hss.cfg
0-59/5 * * * * root     LANG=C /usr/local/mrtg/bin/mrtg /usr/local/mrtg/cfg/ram_hss.cfg
0-59/5 * * * * root     LANG=C /usr/local/mrtg/bin/mrtg /usr/local/mrtg/cfg/cpu_icscf.cfg
0-59/5 * * * * root     LANG=C /usr/local/mrtg/bin/mrtg /usr/local/mrtg/cfg/ram_icscf.cfg
0-59/5 * * * * root     LANG=C /usr/local/mrtg/bin/mrtg /usr/local/mrtg/cfg/cpu_pcscf.cfg
0-59/5 * * * * root     LANG=C /usr/local/mrtg/bin/mrtg /usr/local/mrtg/cfg/ram_pcscf.cfg
0-59/5 * * * * root     LANG=C /usr/local/mrtg/bin/mrtg /usr/local/mrtg/cfg/cpu_scscf.cfg
0-59/5 * * * * root     LANG=C /usr/local/mrtg/bin/mrtg /usr/local/mrtg/cfg/ram_scscf.cfg
0-59/5 * * * * root     LANG=C /usr/local/mrtg/bin/mrtg /usr/local/mrtg/cfg/disk_hss.cfg
0-59/5 * * * * root     LANG=C /usr/local/mrtg/bin/mrtg /usr/local/mrtg/cfg/disk_icscf.cfg
0-59/5 * * * * root     LANG=C /usr/local/mrtg/bin/mrtg /usr/local/mrtg/cfg/disk_pcscf.cfg
0-59/5 * * * * root     LANG=C /usr/local/mrtg/bin/mrtg /usr/local/mrtg/cfg/disk_scscf.cfg
```

Aby boli grafy MRTG generované v pravidelných intervaloch a dáta vždy aktuálne, bolo potrebné nakonfigurovať spútanie jednotlivých skriptov v plánovači úloh cron. V súbore `/etc/crontab/` boli pridané nasledujúce záznamy, ktoré spúšťajú jednotlivé konfiguračné súbory v 5 minútových intervaloch. Ukážka vyhoreného MRTG



Obr. 6.2: Ukážka MRTG grafu.

grafu pre vyťaženie pamäte RAM je zobrazená na obrázku 6.2. V prílohe sú ďalej uvedené ďalšie grafy. MRTG generuje 4 druhy grafov: „**Denný graf**“, ktorý je tvorený v 5 minútových intervaloch, „**Týždňový graf**“ vykresľuje sa každých 30 minút, „**Mesačný graf**“ zaznamenáva zmeny v dvoj hodinovom intervale a „**Ročný graf**“, ktorý je tvorený jedno-dňovým priemerom.

6.4 Implementácia monitorovacieho systému NfSen

Základné predstavenie monitorovacieho nástroja NfSen je uvedené v kapitole 5.2.2. Pre správne fungovanie NFSen je nainštalovať a nakonfigurovať niekoľko dôležitých komponentov a to: samotný **NfSen**, ktorý slúži ako webový frontend a zobrazuje výsledné grafy sieťovej prevádzky. **NFCAPD** (*angl. netflow capture daemon*), ktorý spracováva netflow dáta a výsledky ukladá lokálne do súboru. NFCAPD je spúšťaný automaticky, každých 5 minút a zachytáva traffic na danom rozhraní zariadenia. Ďalším nástrojom je **NFDUMP** (*angl. netflow dump*), ktorý číta netflow dáta zo súbov, uložených pomocou NFCAPD démona. Dôležitým nástrojom je **Softflowd** sonda, ktorá monitoruje sieťovú prevádzku na danom rozhraní. Pre NfSen nutné takisto doinštalovať do sytému perl moduly a knižnice **libio-socket-inet6-perl** a **librrds-perl** obsahujúce RRD nástroje pre vykresľovanie a spracovanie grafov. Keďže je NfSen monitorovací nástroj pracujúci vo webovom rozhraní,

potrebuje k funkčnosti aj webový server a php moduly. Ako webový server bol použitý Apache vo verzii 2.2.16 5.1.3. Architektúra zobrazujúca rozmiestnenie jednotlivých komponentov pre zachytávanie sieťovej prevádzky je zobrazená na obrázku 4.3. [29], [28], [49].

6.4.1 Konfigurácia NfSen

Konfigurácia NfSen prebieha v hlavnom konfiguračnom súbore `nfsen.conf`. Keďže potrebujeme zachytávať traffic na každom core prvku open IMS siete, je potrebné tento súbor upraviť na každom stroji.

```
$\NfSen master config file
$BASEDIR="/usr/local/nfsen";
$HTMLDIR= "/var/www/nfsen"
$VARDIR= "/var/data/nfsen";
$PROFILESTATDIR="${VARDIR}/profiles-stat";
$PROFILEDATADIR="${VARDIR}/profiles-data";
$PREFIX  = '/usr/bin';
$USER = "nfsen";
$WWWUSER = "www-data";
$WWWGROUP = "www-data";
%sources = ('icscf'
=> { 'port' => '9992', 'col' => '#ff0000', 'IP' => 'icscf', 'type' => 'netflow' },
```

V konfiguračnom súbore je musíme nastaviť správne cesty adresárov, do ktorých bude NfSen pristupovať. Parametre `USER`, `WWWUSER` a `WWWGROUP` prideľujú práva jednotlivým vlastníkom. Používateľ „www-data“ má prístup k súborom v adresári `/var/www/` a je zároveň predvoleným užívateľom Apache servera. Parametrom `sources` definujeme názov zdroja, port na ktorom budú zachytávané netflow dáta, IP adresu konkrétneho serveru a farbu výsledného grafu.

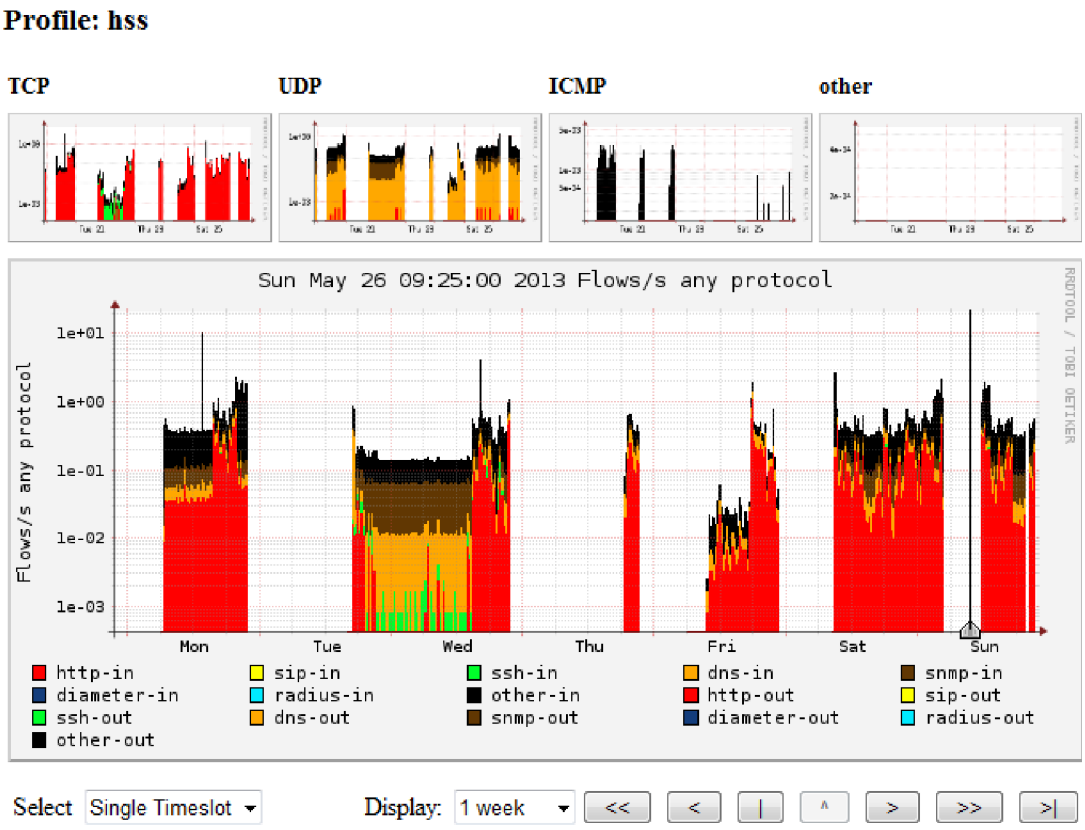
Posledným krokom konfigurácie je vytvoriť skript, pre automatické spúšťanie *softflowd* a *NfSen*. Nasledujúce parametre treba vložiť do súboru `/etc/rc.local`:

```
sudo /bin/mkdir -p /var/run/softflowd/chroot
sudo /usr/sbin/softflowd -i eth0 -n icscf:9992 -p /var/run/sfd.pid.eth0
                                               -c /var/run/sfd.ctl.eth0
sudo /usr/local/nfsen/bin/nfsen start
```

Súbor `/etc/rc.local` sa automaticky spúšťa po štarte operačného systému. Prvý riadok vytvára adresár `chroot`, ktorý vyžaduje *softflowd* sonda. Príkaz v druhom riadku spúšťa *softflowd* sondu na rozhraní „eth0“, serveri „icscf“ a porte „9992“ spolu s PID (*angl. process identifier*) a CTL (*angl. Control*) súbormi. Posledný riadok slúži na spustenie NfSen systému. Nakoniec po reštarte systému a opätovnom nabootovaní môžme pomocou príkazu:

```
ps ax | grep -E "softflowd|nfcapd|nfsen|apache"
```

overiť, či bežia všetky potrebné služby potrebné pre správny chod monitorovacieho nástroja NfSen. Ukážka výsledného grafu pre server HSS je zobrazená na obrázku 6.3. Graf zobrazuje týždennú sieťovú prevádzku na sieťovom rozhraní HSS servera. Jednotlivé medzery medzi intervalmi predstavujú vypnutý server HSS. Keďže celý Open IMS systém je virtualizovaný a pracuje vo virtuálnych strojoch, medzery predstavujú čas, keď bol virtuálny stroj vypnutý. Informácie ohľadom konfigurácie a inštalácie boli čerpané z [30].



Obr. 6.3: Graf sieťovej prevádzky pre HSS.

6.4.2 Vytvorenie profilu NfSen

NfSen ako monitorovací nástroj umožňuje vytvárať vlastné skupiny a profily pre monitorovanie konkrétnych netflow dát. Pre každý z core prvkov siete Open IMS bola vytvorená samostatná skupina s názvom „ims“ a v nej bol vytvorený profil s názvom konkrétneho servera, napr. „icscf“. Ďalej bolo zadefinovaných niekoľko vstupný a výstupných portov na rozhraní daného serveru. Na obrázku 6.4 sú zachytené štatistiky sieťovej prevádzky pre P-CSCF server s konkrétnymi zadefinovanými kanálmi (protokoly: SNMP, RADIUS, SIP a ďalšie). Ako už bolo uvedené v kapitole

4.3.3, administrátor má právo vstupovať do časti profilov a má možnosť si vytvoriť vlastný profil a konfiguráciu prvkov ktoré bude monitorovať. V prílohe A.11 sú uvedené ďalšie obrázky z monitorovacieho systému NfSen. Presný postup na vytváranie nových profilov a možnosti práce so systémom NfSen je uvedený na stránkach [29].

Statistics timeslot May 11 2013 - 17:35

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
other-in	0.5 /s	0.1 /s	0.4 /s	0.0 /s	0 /s	1.8 /s	1.2 /s	0.6 /s	0.0 /s	0 /s	1.7 kb/s	1.3 kb/s	399.4 b/s	9.0 b/s	0 b/s
radius-in	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s
diameter-in	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s
snmp-in	0.1 /s	0 /s	0.1 /s	0 /s	0 /s	0.1 /s	0 /s	0.1 /s	0 /s	0 /s	74.7 b/s	0 b/s	74.7 b/s	0 b/s	0 b/s
dns-in	0.0 /s	0 /s	0.0 /s	0 /s	0 /s	0.0 /s	0 /s	0.0 /s	0 /s	0 /s	56.1 b/s	0 b/s	56.1 b/s	0 b/s	0 b/s
ssh-in	0.1 /s	0.1 /s	0 /s	0 /s	0 /s	1.1 /s	1.1 /s	0 /s	0 /s	0 /s	2.0 kb/s	2.0 kb/s	0 b/s	0 b/s	0 b/s
sip-in	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s
http-in	0.0 /s	0.0 /s	0 /s	0 /s	0 /s	0.3 /s	0.3 /s	0 /s	0 /s	0 /s	1.3 kb/s	1.3 kb/s	0 b/s	0 b/s	0 b/s
http-out	0.0 /s	0.0 /s	0 /s	0 /s	0 /s	0.3 /s	0.3 /s	0 /s	0 /s	0 /s	541.9 b/s	541.9 b/s	0 b/s	0 b/s	0 b/s
sip-out	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s
ssh-out	0.1 /s	0.1 /s	0 /s	0 /s	0 /s	1.1 /s	1.1 /s	0 /s	0 /s	0 /s	1.2 kb/s	1.2 kb/s	0 b/s	0 b/s	0 b/s
dns-out	0.0 /s	0 /s	0.0 /s	0 /s	0 /s	0.0 /s	0 /s	0.0 /s	0 /s	0 /s	15.5 b/s	0 b/s	15.5 b/s	0 b/s	0 b/s
snmp-out	0.1 /s	0 /s	0.1 /s	0 /s	0 /s	0.1 /s	0 /s	0.1 /s	0 /s	0 /s	68.6 b/s	0 b/s	68.6 b/s	0 b/s	0 b/s
diameter-out	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s
radius-out	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s
other-out	0.5 /s	0.1 /s	0.4 /s	0 /s	0 /s	1.9 /s	1.2 /s	0.7 /s	0 /s	0 /s	2.9 kb/s	2.0 kb/s	824.9 b/s	0 b/s	0 b/s
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
TOTAL	1.4 /s	0.5 /s	0.9 /s	0.0 /s	0 /s	6.7 /s	5.2 /s	1.5 /s	0.0 /s	0 /s	9.8 kb/s	8.3 kb/s	1.4 kb/s	9.0 b/s	0 b/s

All None Display: Sum Rate

Obr. 6.4: Štatistiky sieťovej prevádzky pre P-CSCF.

ZÁVER

Cieľom diplomovej práce bolo preštudovať a popísať IMS (IP Multimedia Subsystem) z pohľadu IMS core prvkov a navrhnúť funkčný dohľadový systém pre Open IMS sieť. V prvej kapitole je popísaný stručný prehľad histórie a vzniku IMS subsystému. Sú to popísané jednotlivé IMS core prvky I-CSCF, P-CSCF, S-CSCF a HSS databáza. Každý z týchto prvkov je popísaný z pohľadu funkčnosti v IMS subsystéme. Prvá kapitola sa taktiež venuje popisu signalizácie a rozhraní medzi jednotlivými entitami celého IMS subsystému. Vrámci prvej kapitoly bola popísaná aj architektúra IMS siete.

Kapitola 2 sa venuje popisu dvoch hlavných signalizačných protokolov SIP a DIAMETER a SNMP protokolu, ktorý slúži na výmenu riadiacich informácií medzi zariadeniami pracujúcimi v sieti. V kapitole IMS projekty 3 boli predstavené niekoľké projekty, pracujúce s IMS architektúrou a sieťami novej generácie NGN. Ďalej tu bola zobrazená architektúra Open IMS siete, ktorá predstavuje zároveň jadro školskej experimentálnej IMS siete, pre ktorú bol navrhovaný dohľadový systém.

Výsledkom diplomovej práce je funkčný dohľadový systém Open IMS siete. Na základe teoretickej štúdie bola navrhnutá architektúra dohľadového systému. Na začiatku bol vytvorený a nakonfigurovaný samostatný dohľadový server, na ktorom pracuje dohľadový webový klient, slúžiaci na monitorovanie stavu jednotlivých core prvkov Open IMS siete. Navrhnutý dohľadový systém poskytuje vzdialený prístup ku konfiguračným súborom Open IMS siete, ktoré sú uložené na core prvkoch S-CSCF, P-CSCF, I-CSCF a HSS. Výhodou a prínosom tohto riešenia je možnosť spravovať a nastavovať jednotlivé core prvky školskej experimentálnej IMS siete z jedného miesta.

Ďalej navrhnutý dohľadový systém umožňuje kontrolovať stav zaťaženia procesora, operačnej pamäte a disku každého core prvku a zároveň vykresľovať jednoduché grafy aktuálneho vyťaženia s možnosťou záznamu až 1 rok. Ukážkové grafy možno nájsť v prílohe A.7. Pre zisťovanie a analýzu komunikácie na linkách medzi jednotlivými core prvkami bol nasadený pokročilý monitorovací nástroj. Pre monitorovanie týchto parametrov boli využité open source nástroje MRTG, pre vykresľovanie grafov v časti Status Serverov a NfSen pre vykresľovanie grafov a analýzu sieťovej prevádzky v časti Traffic. NfSen umožňuje vykonávať široké možnosti analýzy sieťových tokov. Bol tu vytvorený vlastný profil s názvom „ims“, v ktorom je možné analyzovať sieťovú prevádzku na konkrétnych portoch core prvkov 6.4.2. Celkový systém pracuje ako jeden celok vo webovom rozhraní.

Prístup k dohľadovému systému je zabezpečený pomocou registrácie užívateľov a prístup ku konfiguračným súborom má len administrátor. Do budúcnosti by mohol byť systém rozšírený o pokročilejšiu prácu s databázou, keďže v aktuálnej verzii slúži databáza iba k registrácii užívateľov. Do databázy by sa mohli ukladať jednotlivé log súbory s dátami získanými z core prvkov Open IMS siete. Log súbory z monitorovania core prvkov sú v aktuálnej verzii dohľadového systému ukladané na lokálny systém dohľadového servera.

ZOZNAM POUŽITEJ LITERATÚRY

[1] *3GPP Specification detail: Architectural requirements [online].* 30. 4. 2004, [cit. 2012-10-30]. Dostupné z: <http://www.3gpp.org/ftp/Specs/html-info/23221.htm>.

[2] *3GPP: Features and contents of each Release [online].* 2012, [cit. 2012-11-11]. Dostupné z: <http://www.3gpp.org/releases>.

[3] *3GPP Specification detail: IP Multimedia Subsystem (IMS), Stage 2 [online].* 2004 [cit. 2012-11-11]. Dostupné z: <http://www.3gpp.org/ftp/Specs/html-info/23228.htm>.

[4] *3GPP Specification detail: Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS), Stage 1 [online].* 30. 4. 2004, [cit. 2012-10-25]. Dostupné z: <http://www.3gpp.org/ftp/Specs/html-info/22228.htm>.

[5] *3GPP Specification detail: Network architecture [online].* 30. 4. 2004, [cit. 2012-11-08]. Dostupné z: <http://www.3gpp.org/ftp/Specs/html-info/23002.htm>.

[6] *Advanced IMS Inc. [online].* 2007-2009 [cit. 2012-12-12]. Dostupné z: <http://advancedims.com/index.html>.

[7] *AMPS [online].* [cit. 2012-12-12]. Dostupné z: <http://advancedims.com/IMS/amps.html>.

[8] *Apache [online].* [cit. 2012-05-07]. Dostupné z: <http://httpd.apache.org/ABOUT_APACHE.html>.

[9] *Debian [online].* [cit. 2012-05-07]. Dostupné z: <http://www.debian.org/>.

[10] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS.* 5. aktualiz. vyd. Brno: Computer Press, a. s., 2008. 489 s. ISBN 978-80-251-2236-5.

[11] *FOKUS Home Subscriber Server (FHoSS) [online].* [cit. 2012-12-05]. Dostupné z: <http://www.fokus.fraunhofer.de/en/fokus_testbeds/open_ims_playground/components/osims/fhoss/index.html>.

[12] GIGEL, Milan. *Ako na MRTG I - Príprava, inštalácia, prvý graf [online].* 2002-10-14 [cit. 2013-05-26]. Dostupné z: <http://www.linuxzone.cz/index.phtml?idc=408&ids=29>.

[13] *H.248.1: Gateway control protocol: Version 3. ITU-T Recommendations [online].* Geneva: International Telecommunication Union, 2000 [cit. 2012-11-17]. Dostupné z: <http://www.itu.int/rec/T-REC-H.248.1-200509-I/en>.

[14] HARRISON, Peter. *Linux Home Networking [online].* 2012 [cit. 2013-05-21]. Dostupné z: <http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch22_:_Monitoring_Server_Performance#.UaEixtsy5uD>.

[15] *IMS Zone [online].* 2009 [cit. 2012-12-12]. Dostupné z: <http://www.imszone.org/>.

[16] *Kamailio – the Open Source SIP Server [online].* 2001-2010 [cit. 2012-12-07]. Dostupné z: <http://www.kamailio.org/w/>.

[17] *Kamailio – Features [online].* 2001-2010 [cit. 2012-12-07]. Dostupné z: <http://www.kamailio.org/w/features/>.

[18] *littleIMS [online].* 28.10.2009 [cit. 2012-12-11]. Dostupné z: <http://confluence.cipango.org/display/LITTLEIMS/Home>.

[19] LIU, Jeffrey, JIANQ, Steven, LIN, Hicks. *The Introduction to Diameter. Get the next generation AAA protocol [online].* 2006 [cit. 2012-12-01]. Dostupné z: <http://www.ibm.com/developerworks/library/wi-diameter/index.html

[20] MOGHADAM, Pejman. *Using MRTG for CPU, memory and hard disk usage of Linux [online].* 2009-04-25 [cit. 2013-05-26]. Dostupné z: <http://www.pmoghadam.com/homepage/HTML/MRTG-cpu-mem-hdd-linux.html>.

[21] *MVC aplikace & presentery [online].* [cit. 2013-05-16]. Dostupné z: <http://doc.nette.org/cs/presenters>.

[22] *MySQL [online].* 1995-2012 [cit. 2012-12-08]. Dostupné z: <http://www.mysql.com/>.

[23] *NGNLAB [online].* [cit. 2012-12-08]. Dostupné z: <http://www.ngnlab.eu/index.php/about-ngnlabeu>.

[24] *NGNLAB – Live CD [online].* [cit. 2012-12-09]. Dostupné z: <http://www.ngnlab.eu/index.php/projects/ngn-lab-projects/111-openimscore-livecd>

[25] *July 2012 Web Server Survey [online].* [cit. 2013-05-07]. Dostupné z: <http://news.netcraft.com/archives/2012/07/03/july-2012-web-server-survey.html>.

[26] *NET-SNMP Tutorial [online].* 2011 [cit. 2013-05-18]. Dostupné z: <http://net-snmp.sourceforge.net/tutorial/tutorial-5/mrtg/>.

[27] *Nette [online].* [cit. 2013-05-16]. Dostupné z: <http://nette.org/cs/>.

[28] *NFDUMP [online].* [cit. 2013-05-22]. Dostupné z: <http://nfdump.sourceforge.net/>.

[29] *NfSen - Netflow Sensor [online].* [cit. 2013-05-22]. Dostupné z: <http://nfsen.sourceforge.net/>.

[30] NOVÁK, Filip. *Softflowd + NFDUMP + NfSen - instalace a konfigurace [online].* 2012-01-20 [cit. 2013-05-26]. Dostupné z: <http://www.filipnovak.com/linux/ubuntu/softflowd-nfdump-nfsen-instalace-a-konfigurace>.

[31] OETIKER, Tobias. *MRTG Multi Router Traffic Grapher [online].* [cit. 2013-05-21]. Dostupné z: <http://oss.oetiker.ch/mrtg/doc/mrtg.en.html>.

[32] *OSIMS: The FOKUS Open Source IMS Core [online].* 2004-2008 [cit. 2012-12-01]. Dostupné z: <http://www.fokus.fraunhofer.de/en/fokus_testbeds/open_ims_playground/components/osims/index.html>.

[33] *Open Source IMS [online].* 2004-2008 [cit. 2012-12-01]. Dostupné z: <http://openimscore.org/>.

[34] *OpenIMSCore in a VM [online].* 2004-2008 [cit. 2012-12-02]. Dostupné z: <http://openimscore.org/vm>.

[35] *PHP [online].* 2001-2012 [cit. 2012-12-09]. Dostupné z: <http://us.php.net/>.

[36] POIKSELKA, M., MAYER, G., *The IMS: IP Multimedia Concepts and Services.* V. Británia: WILEY, 2009. 560 s. Tretie vydanie. ISBN 978-0-470-72196-4.

[37] RUSSELL, T., *The IP Multimedia Subsystem (IMS): Session Control and Other Network Operations.* V. Británia: Mc Graw-Hill OSBOURNE, 2008. 242 s. ISBN 0071488537.

[38] *RFC 3261: SIP Session Initiation Protocol [online].* [cit 2012-11-23]. Dostupné z: <http://www.ietf.org/rfc/ rfc3261.txt>.

[39] *RFC 822: Strandard for the format of ARPA internet text messages [online].* [cit 2012-11-23]. Dostupné z: <http://www.faqs.org/rfcs/ rfc822.html>.

[40] *RFC 2976: The SIP INFO Method [online].* [cit 2012-11-28]. Dostupné z: <http://www.ietf.org/rfc/rfc2976.txt>.

[41] *RFC 3311: The Session Initiation Protocol (SIP) UPDATE Method [online].* [cit 2012-11-29]. Dostupné z: <http://www.ietf.org/rfc/rfc2976.txt>.

[42] *RFC 6733: Diameter Base Protocol [online].* [cit 2012-11-29]. Dostupné z: <http://tools.ietf.org/html/rfc6733>.

[43] *RFC 1155: Structure and Identification of Management Information for TCP-IP-based Internets [online].* [cit 2012-12-02]. Dostupné z: <http://www.ietf.org/rfc/rfc1155.txt>.

[44] *RFC 1157: A Simple Network Management Protocol (SNMP) [online].* [cit 2012-12-02]. Dostupné z: <http://www.ietf.org/rfc/rfc1157.txt>.

[45] *RFC 1902: Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2) [online].* [cit 2012-12-04]. Dostupné z: <http://tools.ietf.org/html/rfc1902>.

[46] SALEKUL, Islam, Grégoire JEAN-CHARLES. *Computer Networks: Multi-domain authentication for IMS services [online].* Zväzok 55, vydanie 12. Amsterdam: Elsevier, 25 August 2011, s. 2689-2704 [cit. 2012-11-10]. ISBN 1389-1286. Dostupné z: <http://www.sciencedirect.com/science/article/pii/S1389128611001423>.

[47] *Simple Network Management Protocol [online].* 16.10.2012 [cit. 2012-12-02]. Dostupné z: <http://docwiki.cisco.com/wiki/Simple_Network_Management_Protocol>.

[48] *Simple Network Management Protocol Version 3 [online].* [cit. 2012-12-04]. Dostupné z: <http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html>.

[49] *Softflowd [online].* 16.10.2012 [cit. 2012-12-02]. Dostupné z: <http://code.google.com/p/softflowd/>.

[50] SULTAN, Philippe. *SIP peers external authentication in Asterisk / OpenPBX [online].* 2006 [cit. 2012-12-01]. Dostupné z: <https://who.rocq.inria.fr/Philippe.Sultan/Asterisk/asterisk_sip_external_authentication.html>.

[51] *Ubuntu wiki [online].* [cit 2013-05-07]. Dostupné z: <https://wiki.ubuntu.com/LTS>.

[52] *VirtualBox [online].* [cit 2013-05-08]. Dostupné z: <https://www.virtualbox.org/>.

ZOZNAM SYMBOLOV, VELIČIN A SKRATIEK

3GPP	3rd Generation Partnership Project
AMPS	Asynchronous Middleware for Protocol Servers
AAA	Authentication, Authorization and Accounting
AS	Application Server
AJAJ	Asynchronous JavaScript and JSON
AJAX	Asynchronous JavaScript and XML
ASP	Active Server Pages
AuC	Authentication Center
AVP	Attribute-Value Pairs
BGCF	Breakout Gateway Control Function
CAMEL	Customized Applications for Mobile Network Enhanced Logic
CDR	Call Detail Records
CDMA	Code Division Multiple Access
CFML	ColdFusion Markup Language
COPS	Common Open Policy Service
CPU	Central Processing Unit
CS	Circuit Switched
CSS	Cascading Style Sheets
CSCF	Call Session Control Function
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specification
DSL	Digital Subscriber Line
E-CSCF	Emergency CSCF
EDGE	Enhanced Data Rates for Global Evolution

FHoSS	FOKUS Home Subscriber Server
GGSN	Gateway GPRS Support Node
GPL	General Public License
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
IBCF	Interconnection Border Control Function
I-CSCF	Interrogating CSCF
ICS	IMS Service Control Reference Point
IETF	Internet Engineering Task Force
IIS	Internet Information Services
IM	Instant Messaging
IM-SSF	IP Multimedia Service Switching Function
IM-MGW	IMS Media GateWay
IMAP	Internet Message Access Protocol
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPsec	Internet Protocol security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISC	IMS Service Control Reference Point
ISDN	Integrated Services Digital Network

ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
JSON	JavaScript Object Notation
JSP	JavaServer Pages
LCS	Location Services
LDAP	Lightweight Directory Access Protocol
LRF	Location Routing Function
LTE	Long Term Evolution
LTS	Long Term Support
MAP	Mobile Application Part
MGCF	Media Gateway Controller Function
MGW	Media Gateway
MIB	Management Information Base
MRB	Media Resource Broker
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
MRTG	Multi Router Traffic Grapher
MSISDN	Mobile Subscriber International ISDN Number
MSC	Mobile Switching Centre
MVC	Model-View-Controller
NGN	Next Generation Network
NMS	Network Management System
OSA	Open Services Architecture
P-CSCF	Proxy CSCF
PDF	Policy Decision Function

PNG	Portable Network Graphics
PoC	Push to talk over the Cellular service
POP3	Post Office Protocol
PS	Packet Switched Presence Server
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
RAM	Random Access Memory
RFC	Request for Comments
RMDBS	Relational Database Management System
RPC	Remote Procedure Call
RRD	Round Robin Database
RTP	Real-Time Transport Protocol
RTSP	Real-Time Streaming Protocol
QoS	Quality of Service
S-CSCF	Serving CSCF
SA	Security Associations
SAE	System Architecture Evolution
SBLP	Service-Based Local Policy
SCS	Service Capability Server
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SEO	Search engine optimization
SER	SIP Express Router
SGSN	Serving GPRS Support Node

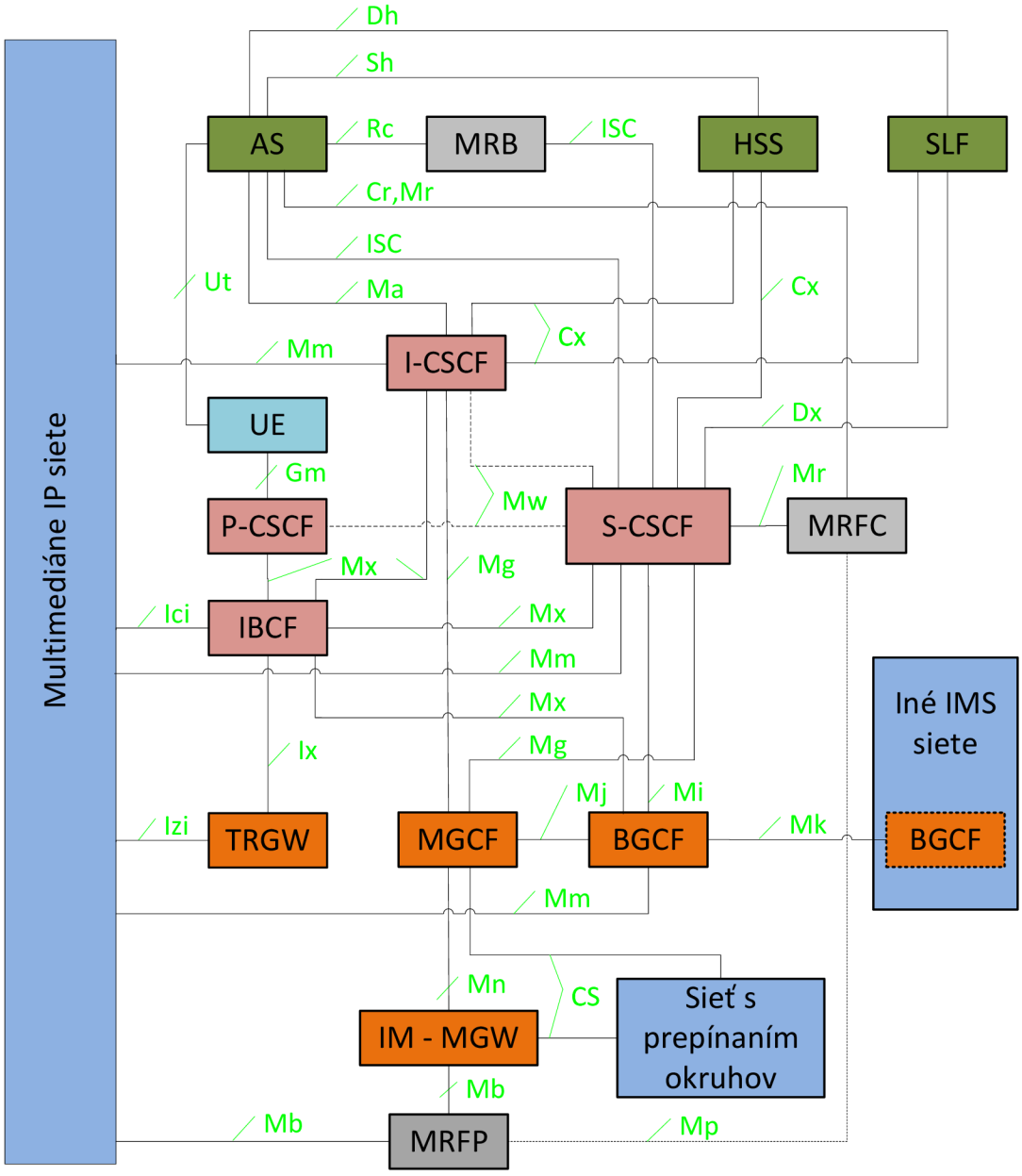
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SMP	Simple Management Protocol
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SRVCC	Single Radio Voice Call Continuity
SSH	Secure Shell
SQL	Structured Query Language
TCP	Transmission Control Protocol
THIG	Topology Hiding Inter-network Gateway
TISPAN	Telecommunications and Internet coverged Services and Protocols for Advanced Networking
TLS	Transport Layer Security
TrGW	Transition Gateway
UDP	User Datagram Protocol
UDR	User Deails Records
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
URI	Universal Resource Identifier
URL	Uniform Resource Locator
USSD	Unstructured Supplementary Service Data
UTRAN	UMTS Terrestrial Radio Access Network
VoD	Video on Demand
WLAN	Wireless Application Protocol
XHTML	Extensible HyperText Markup Language

XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

ZOZNAM PRÍLOH

A PRÍLOHA

A.1 IMS architektúra z pohľadu rozhraní a entít



Obr. A.1: IMS architektúra z pohľadu rozhraní a entít [36].

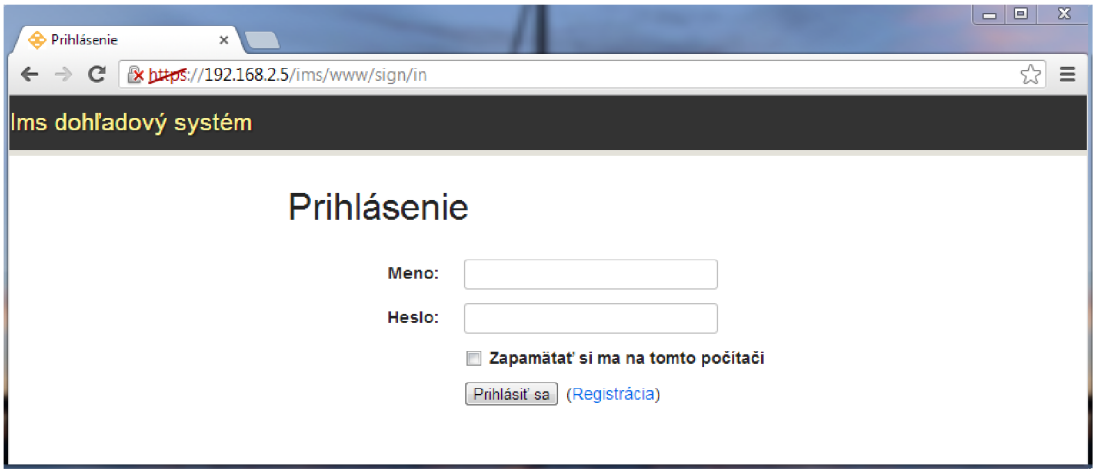
A.2 Tabuľka s prihlasovacími údajmi

Tab. A.1: Prihlasovacie údaje.

Dohľadový systém	
meno	admin
heslo	imsDS13
Core prvky Open IMS siete	
meno	ims
heslo	ims1net2
Dohľadový server	
meno	root
heslo	server78
meno	michal
heslo	svec12*
Databáza (phpMyAdmin)	
meno	ims
heslo	imsphp

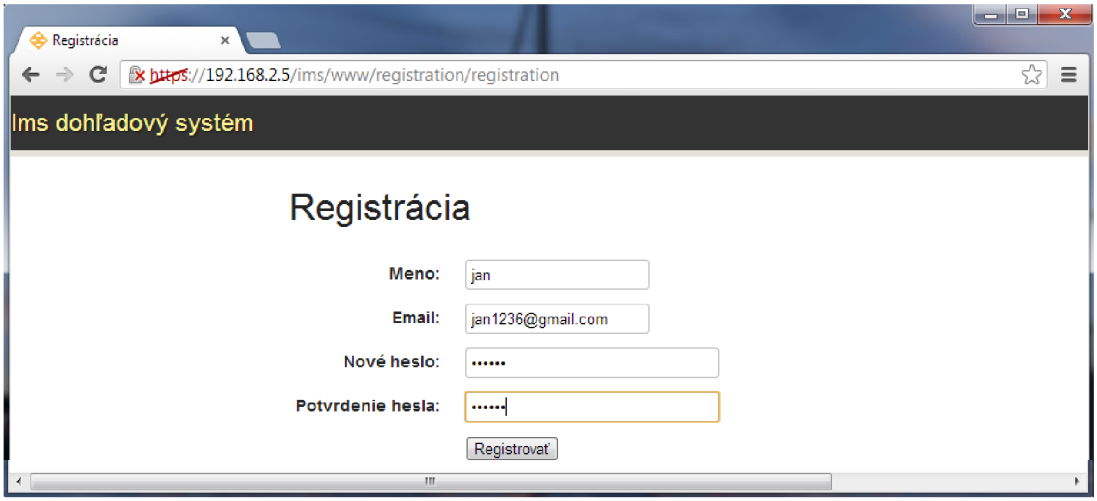
Tabuľka A.1 obsahuje prihlasovacie údaje pre prístup do dohľadového systému s administrátorskými právami. Ďalej obsahuje prihlasovacie údaje do operačného systému core prvkov P-CSCF, S-CSCF, I-CSCF a HSS spolu s prihlasovacími údajmi na dohľadový server. Posledná položka tabuľky obsahuje prístupové údaje do navrhnutej databáze.

A.3 Prihlasovacia obrazovka



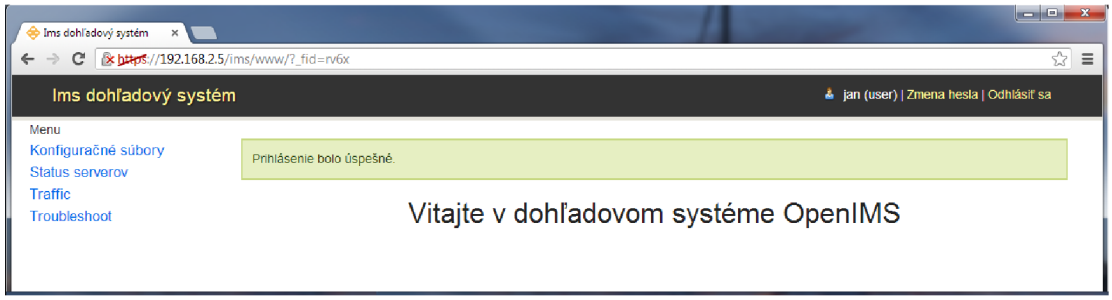
Obr. A.2: Prihlasovacia obrazovka.

A.4 Registračná obrazovka



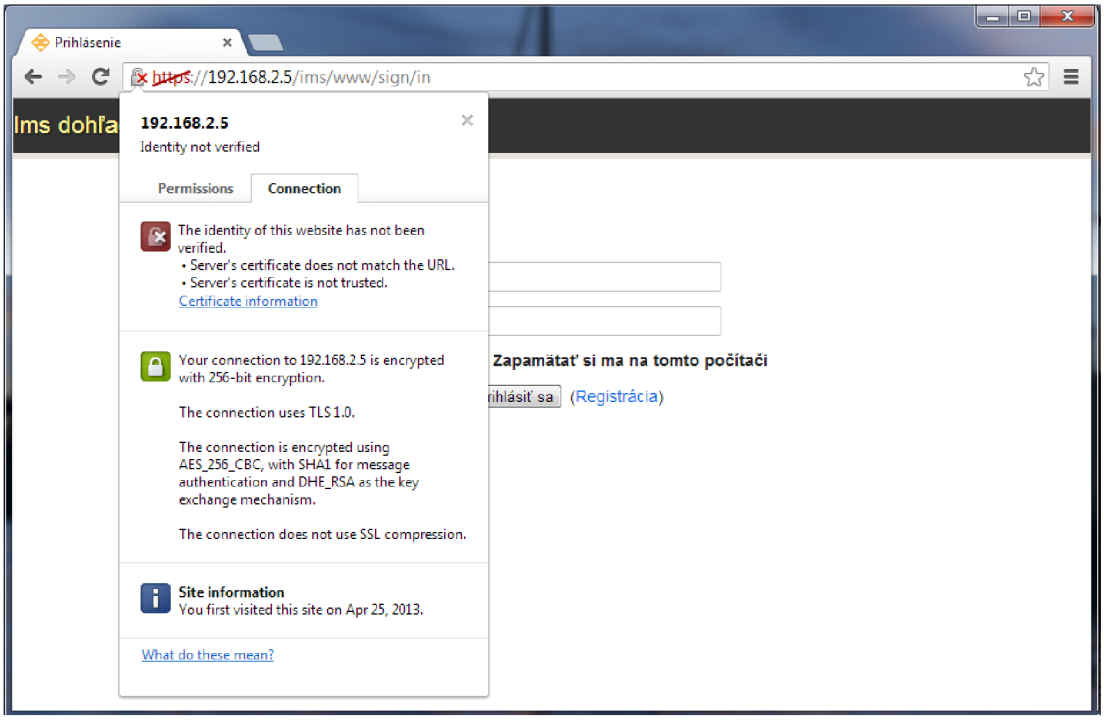
Obr. A.3: Registračná obrazovka.

A.5 Úvodná obrazovka po úspešnom prihlásení



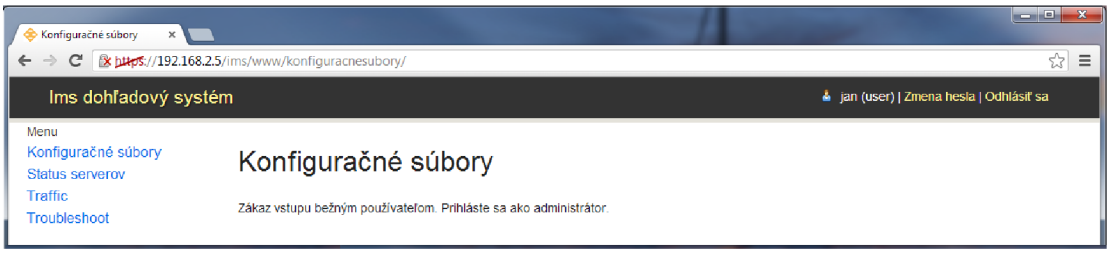
Obr. A.4: Úvodná obrazovka po úspešnom prihlásení.

A.6 Šifrovaný prenos dát



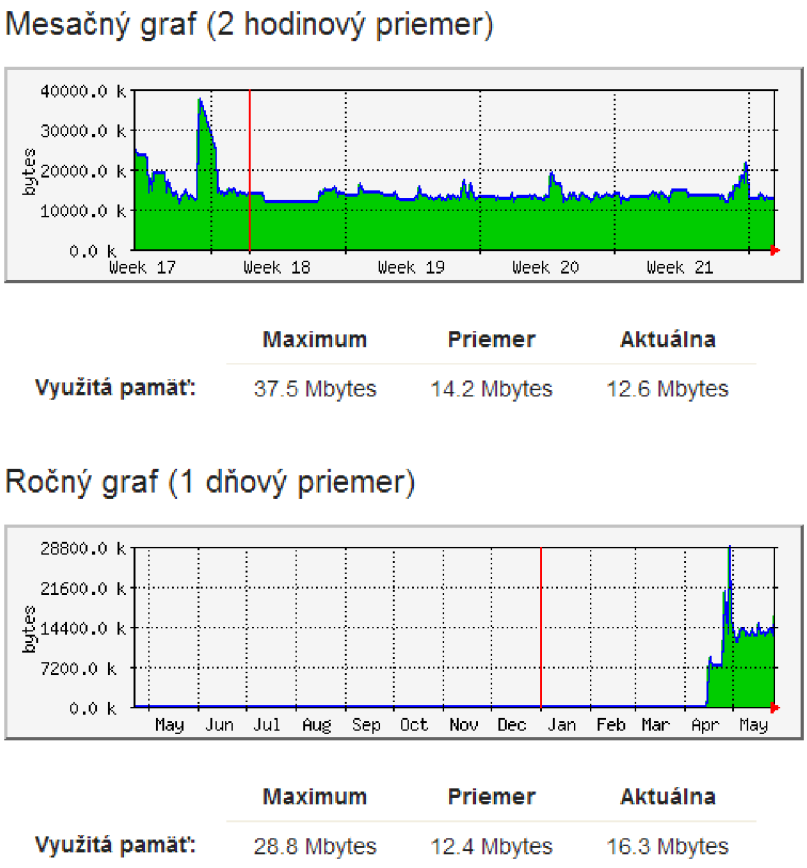
Obr. A.5: Šifrovaný prenos dát.

A.7 Obmedzenie prístupu



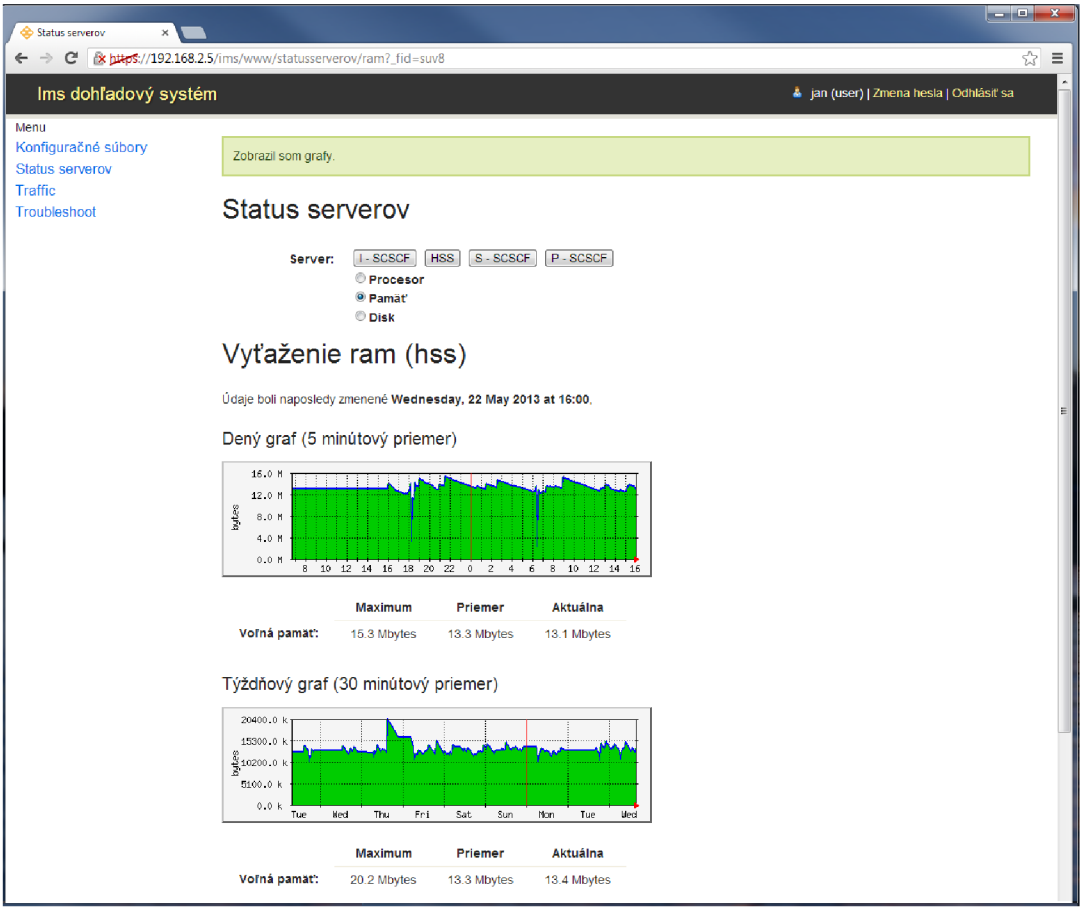
Obr. A.6: Obmedzenie prístupu.

A.8 Ročný a mesačný graf využitia RAM (HSS)



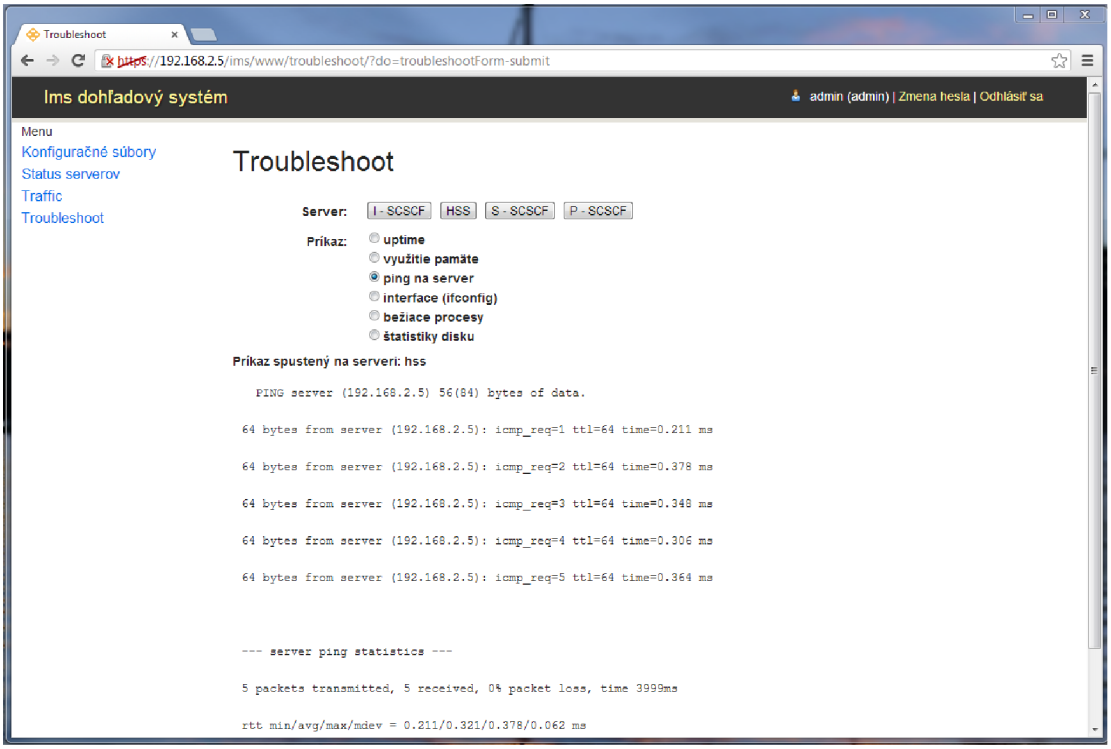
Obr. A.7: Ročný a mesačný graf využitia RAM (HSS).

A.9 Graf vyťaženia RAM (HSS)



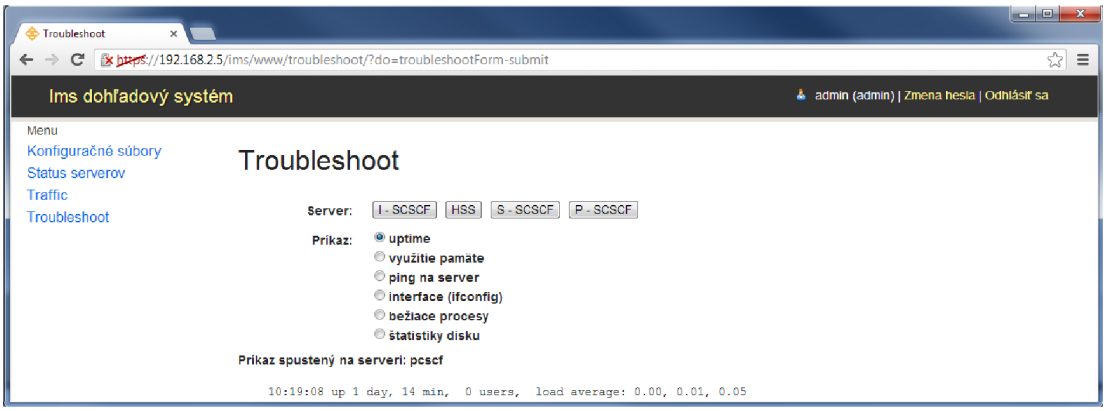
Obr. A.8: Graf vyťaženia RAM (HSS).

A.10 Troubleshoot - ping na server



Obr. A.9: Troubleshoot - ping na server.

A.11 Troubleshoot - uptime servera

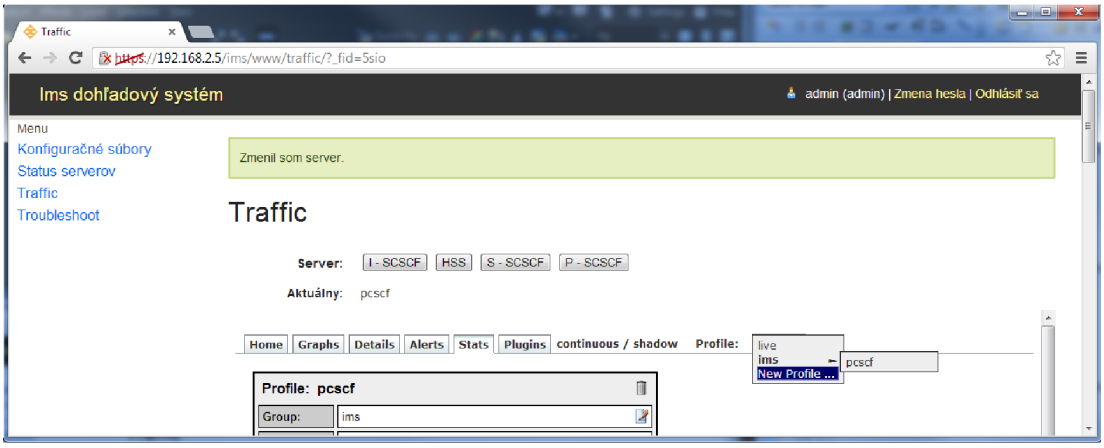


Obr. A.10: Troubleshoot - uptime servera.

A.12 Traffic (P-CSCF)

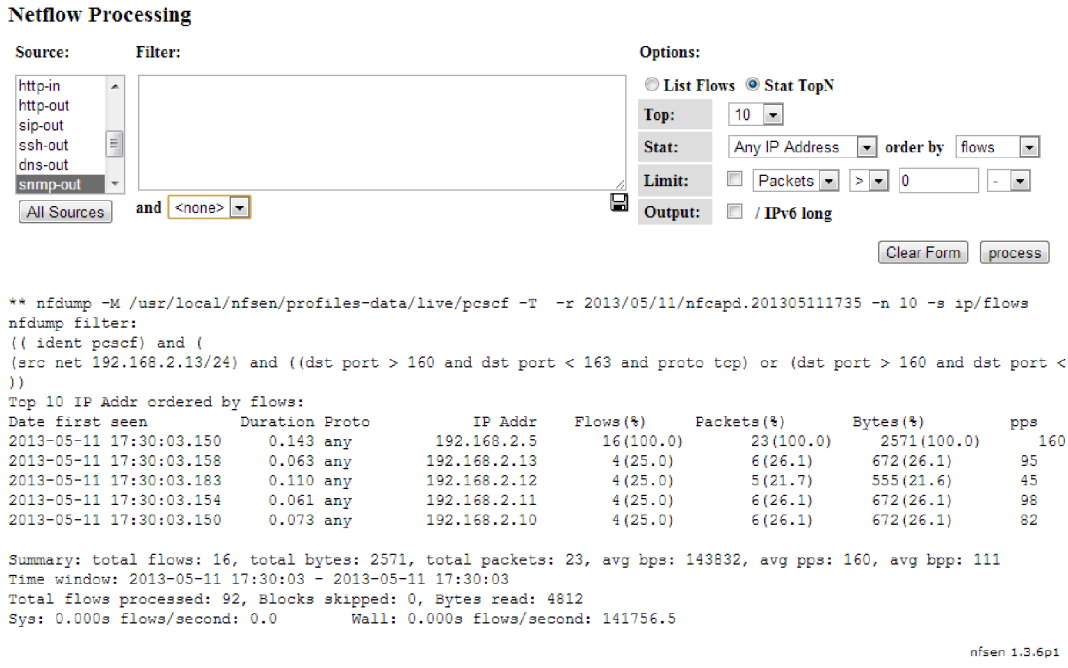
Obr. A.11: Traffic (P-CSCF).

A.13 Tvorba nového profilu



Obr. A.12: Tvorba nového profilu.

A.14 Spracovanie Netflow dát



Obr. A.13: Spracovanie Netflow dát.

B KONFIGURAČNÉ SÚBORY MRTG

B.1 Konfiguračný súbor pre I-CSCF (CPU)

```
WorkDir: /var/www/ims/www/mrtg/icscf/
Refresh: 300

LoadMIBs: /usr/local/share/snmp/mibs/UCD-SNMP-MIB.txt
Target[cpu_icscf]:ssCpuRawUser.0&ssCpuRawUser.0:public@icscf+
ssCpuRawSystem.0&ssCpuRawSystem.0:public@icscf+
ssCpuRawNice.0&ssCpuRawNice.0:public@icscf
RouterUptime[cpu_icscf]: public@icscf
MaxBytes[cpu_icscf]: 100
Title[cpu_icscf]: CPU Load
PageTop[cpu_icscf]: <H1>Active CPU Load %</H1>
Unscaled[cpu_icscf]: ymwd
ShortLegend[cpu_icscf]: %
YLegend[cpu_icscf]: CPU Zataz
Legend1[cpu_icscf]: Active CPU in % (Load)
Legend2[cpu_icscf]:
Legend3[cpu_icscf]:
Legend4[cpu_icscf]:
LegendI[cpu_icscf]: Active
LegendO[cpu_icscf]:
Options[cpu_icscf]: growright,nopercent
```

B.2 Konfiguračný súbor pre HSS (RAM)

```
WorkDir: /var/www/ims/www/mrtg/hss/
LoadMIBs: /usr/local/share/snmp/mibs/HOST-RESOURCES-MIB.txt
Refresh: 300

Target[ram_hss]: .1.3.6.1.4.1.2021.4.6.0&
.1.3.6.1.4.1.2021.4.6.0:public@hss
PageTop[ram_hss]: <H1>Free Memory</H1>
Options[ram_hss]: nopercent,growright,gauge,noinfo
Title[ram_hss]: Volna pamat
MaxBytes[ram_hss]: 100000000000
kMG[ram_hss]: k,M,G,T,P,X
YLegend[ram_hss]: bytes
ShortLegend[ram_hss]: bytes
LegendI[ram_hss]: Free Memory:
LegendO[ram_hss]:
Legend1[ram_hss]: Free memory, not including swap, in bytes
```

B.3 Konfiguračný súbor pre P-CSCF (HDD)

```
WorkDir: /var/www/ims/www/mrtg/pcscf/
Refresh: 300

LoadMIBs: /usr/local/share/snmp/mibs/UCD-SNMP-MIB.txt
Target[disk_pcscf]:dskPercent.1&dskPercent.2:public@pcscf
Title[disk_pcscf]: Disk Partition Usage
PageTop[disk_pcscf]: <H1>Disk Partition Usage /home and /var</H1>
MaxBytes[disk_pcscf]: 100
ShortLegend[disk_pcscf]: %
YLegend[disk_pcscf]: Zataz
LegendI[disk_pcscf]: /home
LegendO[disk_pcscf]: /var
Options[disk_pcscf]: gauge,growright,nopercent
Unscaled[disk_pcscf]: ymwd
```

C OBSAH PRILOŽENÉHO CD

Priložený disk obsahuje nasledujúce súbory:

- `/doc/diplomova-praca.pdf` - text diplomovej práce vo formáte PDF
- `/src/Open_IMS/` - konfiguračné súbory core prvky (P-CSCF, S-CSCF, I-CSCF a HSS)
- `/src/Server/` - konfiguračné súbory použité na dohľadovom serveri
- `/core_P-CSCF/image.virtualbox` - image disku P-CSCF core prvku
- `/core_I-CSCF/image.virtualbox` - image disku I-CSCF core prvku
- `/core_S-CSCF/image.virtualbox` - image disku S-CSCF core prvku
- `/core_HSS/image.virtualbox` - image disku HSS core prvku
- `/core_Server/image.virtualbox` - image disku dohľadového servera