

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

METODIKA TESTOVÁNÍ IP MULTIMEDIA SUBSYSTEM

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

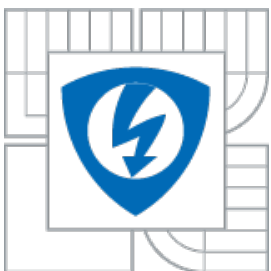
MARTIN KARLÍK

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

Metodika testování IP Multimedia Subsystem

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

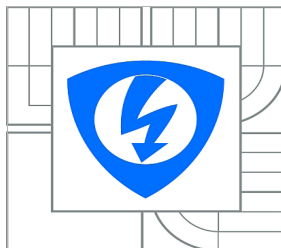
AUTOR PRÁCE
AUTHOR

MARTIN KARLÍK

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. L'UBOŠ NAGY

BRNO 2013



VYSOKÉ UČENÍ
TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor

Teleinformatika

Student: Martin Karlík
Ročník: 3

ID: 136535
Akademický rok: 2012/2013

NÁZEV TÉMATU:

Metodika testování IP Multimedia Subsystem

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je prostudovat a popsat subsystém IMS (IP Multimedia Subsystem) z pohledu aplikační vrstvy. V rámci práce se také seznámte se standardem o metodice testování IMS sítě pro tvorbu test-bedu služby sledování dostupnosti klientu poskytované prostřednictvím aplikačního serveru. Navrhnete architekturu test-bedu (reálné implementaci testované architektury založené na open source) a definujete způsob analýzy dat, které budou výsledkem výkonostního testování jednotlivých prvků navrhnuté sítě. Navržen test-bed zrealizujete.

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.
- [3] 3rd Generation Partnership Project. Presence services: Architecture and functional description. 3GPP TS 23.141. 2011.

Termín zadání: 11.2.2013

Termín odevzdání: 5.6.2013

Vedoucí práce: Ing. Ľuboš Nagy
Konzultanti bakalářské práce:

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

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následku porušení ustanovení § 11 a následujících autorského zákona c. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku c.40/2009 Sb.

ABSTRAKT

Karlík, Martin

Ústav telekomunikací, Fakulta elektrotechniky a komunikačních technologií, Vysoké učení technické v Brně.

Metodika testovania IP Multimedia Subsystem

Cieľom tejto práce je štúdium, rozbor, opis a realizácia architektúry IMS siete a výkonnostného testovania siete na základe RFC 6076, tj. pri komunikácii s koncovými terminálmi cez prvky P-CSCF, I-CSCF, S-CSCF, HSS. Merané sú metriky definované v štandarde RFC 6076 pre SIP protokol. Meranie bolo vykonané pri vytváraní relácie medzi dvomi terminálmi a prihlasovaní do siete pri rôznej záťaži CPU a RAM pamäte. Ďalej je práca zameraná na implementáciu samotnej IMS siete založenej na Open Source SIP Server Kamalio, Open IMS Core a Open Source IMS Core System FhoSS.

KLÚČOVÉ SLOVÁ

IMS, CSCF, SIP, HSS, IMS architektúra, RFC 6076, test-bed, kamailio

ABSTRACT

Karlík, Martin

Department of Telecommunications, Faculty of Electrical Engineering and Communication, Brno University of Technology.

Methodology for testing IP Multimedia Subsystem

The aim of this work is the study, analysis and description of the IMS network architecture and performance testing based on RFC 6076, i.e communication with end terminals via elements P-CSCF, S-CSCF, I-CSCF, HSS. Measured are metrics defined in standard RFC 6076 for SIP protocol. Measuring was realized when terminal is registering into network and creating a session between two terminals using SIP INVITE and REGISTER and systems are under various load of CPU and RAM memory. Further project is focused on the implementation of the IMS network based on the Open Source SIP Server Kamalio, Open IMS Core and Open Source IMS Core System FhoSS.

KEY WORDS

IMS, CSCF, SIP, HSS, IMS architecture, RFC 6076, test-bed, kamailio

KARLÍK, M. *Metodika testování IP Multimedia Subsystem*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2013. 88 s. Vedoucí bakalářské práce Ing. Ľuboš Nagy.

PREHLÁSENIE

Prehlasujem, že som svoj semestrálny projekt na tému „Metodika testovania IP Multimedia Subsystem“ vypracoval samostatne pod vedením vedúceho semestrálneho projektu, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedeného semestrálneho projektu ďalej prehlasujem, že v súvislosti s vytvorením tohoto semestrálneho projektu som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia §11 a nasledujúcich autorského zákona č. 121/2000Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), vo znení neskorších predpisov, vrátane možných trestnoprávných dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka č.40/2009 Sb.

Brno

.....
(podpis autora)

POĎAKOVANIE

Rád by som sa poďakoval vedúcemu bakalárskej práce pánovi Ing. Ľubošovi Nagyovi za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.

Brno

.....
(podpis autora)

POĎAKOVANIE

Výskum popísaný v tomto semestrálnom projekte bol realizovaný v laboratóriách podporených z projektu SIX; registračné číslo CZ.1.05/2.1.00/03.0072, operační program Výskum a vývoj pre inovácie.

Brno

.....
(podpis autora)

OBSAH

Úvod.....	11
1 Požiadavky na IMS	12
2 Protokoly v IMS	12
2.1 Protokoly riadenia spojov.....	12
2.1.1 BICC (Bearer Independent Call Control)	13
2.1.2 H.323	13
2.1.3 SIP (Session Initiation Protocol), RFC 3261	13
2.1.4 RTP (Real-time Transport Protocol).....	15
2.1.5 SDP (Session Description protocol).....	15
2.2 AAA protokol.....	16
2.2.1 DIAMETER.....	16
3 Architektúra IMS	17
3.1 Blok riadenia a smerovania relácií.....	17
3.1.1 P-CSCF (Proxy Call Session Control Function).....	17
3.1.2 I-CSCF (Interrogating Call Session Control Function).....	18
3.1.3 S-CSCF (Serving Call Session Control Function).....	18
3.1.4 E-CSCF (Emergency Call Session Control Function).....	19
3.2 Blok Služieb poskytovaných užívateľom.....	19
3.2.1 SIP aplikačný server.....	20
3.2.2 OSA-SCS (Open Service Access-Service Capability Server).....	20
3.2.3 IM-SSF (IP Multimedia Service Switching Function).....	20
3.2.4 Aplikačný server ako SIP User Agent	20
3.2.5 Aplikačný server ako SIP Proxy Server.....	20
3.2.6 Aplikačný server ako SIP Redirect Server	21
3.2.7 Aplikačný server ako SIP B2BUA	21
3.2.8 MRF (Media Resource Function).....	21
3.2.9 MRFC (Media Resource Function Controller).....	22
3.2.10 MRFP (Media Resource Function Controller).....	22
3.2.11 Initial Filter Criteria.....	22
3.3 Databázy.....	24
3.3.1 Databázy HSS a SLF	24
3.4 Služby zabezpečujúce medzi-sieťovú komunikáciu.....	24
3.4.1 BGCF (Breakout Gateway Control Function).....	24
3.4.2 IMS-ALG (Application Layer Gateway) a TrGW (Translation Gateway).....	24
3.4.3 SGW (Signaling Gateway).....	25
3.4.4 MGCF (Media Gateway Control Function).....	25
3.4.5 MGW (Media Gateway).....	25
4 Prezenčné služby	26
4.1 Prezenčné informácie – formát dát	27
4.2 Prezenčné služby v IMS	28
4.2.1 Presence server	28
4.2.2 Resource List Server	28
4.2.3 XDMS (XML Document Management Servers)	28
4.2.4 XCAP (XML Configuration Access Protocol).....	28
4.2.5 Content server	29
4.2.6 Presence source	29

4.2.7 Presence watcher	29
4.2.8 Watcher agent	29
4.3 Zverejnenie prezenčných informácií.....	30
4.4 Získanie prezenčných informácií.....	31
4.5 Poskytnutie informácií o watcheroch.....	33
5 IMS/TISPAN NGN výkonnostný test.....	35
5.1 Test – Bed	36
5.2 SUT (System Under Test).....	36
5.2.1 Základňa užívateľov.....	37
5.2.2 SUT parametre a konfigurácia.....	37
5.3 TS (Test System).....	37
5.3.1 TS parametre a konfigurácia.....	37
5.4 Zaznamenávané parametre výkonnostného testu	38
5.4.1 IMS/KPI Úspešnosť počiatočnej registrácie S – CSCF.....	38
5.4.2 IHS (Inadequately Handled Scenario) parameter	38
5.5 Vlastná architektúra IMS siete a test – bedu.....	38
5.5.1 Ixia LxLoad.....	38
5.5.2 Kamailio open source SIP server.....	39
5.5.3 Umelá záťaž CPU	39
5.5.4 FHoSS Open IMS Core.....	39
5.5.5 OpenXCAP.....	40
5.5.6 Popis navrhutej architektúry IMS siete a test-bedu.....	40
5.5.7 Priebeh meraní.....	44
6 Inštalácia, chyby pri inštalácii a oživovaní IMS siete	46
6.1 Kamailio Open source SIP server.....	46
6.1.1 Inštalácia.....	46
6.1.2 Chyby pri spúšťaní P-CSCF	47
6.1.3 Spustenie S – CSCF	48
6.1.4 Spustenie I – CSCF	48
6.1.5 Nefunkčnosť Prezenčného a XCAP serveru.....	49
6.2 Open IMS Core.....	51
6.2.1 Inštalácia	51
6.2.2 Chyba prezenčného servera Opensips.....	51
7 Boghe IMS klient.....	53
8 Metodika testovania	54
8.1 Hardvérové a softvérové parametre serverov.....	54
8.1.1 Hardvér.....	54
8.1.2 Operačný systém a softvér.....	54
8.1.3 Nastavovanie umelej záťaže	54
8.1.4 Nastavenie generátora	55
8.1.5 Wireshark.....	55
8.2 Tok správ a porovnanie časov pri prihlasovaní a vytváraní relácie.....	55
8.2.1 Testované scenáre.....	55
8.3 Výsledky meraní.....	57
8.3.1 Internet Engineering Task Force (IETF) RFC 6076.....	57
8.3.2 Registration Request Delay (RRD).....	57
8.3.3 Ineffective registration attempts (IRAs).....	61
8.3.4 Session request delay bez presmerovania (SRD).....	61
8.3.5 Ineffective session attempts (ISAs).....	64
8.3.6 Call setup time.....	65

8.3.7 Media Delay.....	68
8.3.8 Post Pick up delay.....	71
8.3.9 Session Disconnect Delay (SDD).....	74
9 ZÁVER.....	78
10 LITERATÚRA.....	80
11 ZOZNAM ZKRATIEK.....	83

Zoznam obrázkov

Obrázok 1: Protokoly v IMS [6].....	12
Obrázok 2: SDP [6].....	15
Obrázok 3: Vzťah medzi základným protokolom a jeho aplikáciami[6].....	16
Obrázok 4: Architektúra IMS.....	17
Obrázok 5: Route field [6].....	21
Obrázok 6: SIP B2B UA[6].....	21
Obrázok 7: Initial Filter Criteria[6].....	22
Obrázok 8: Informácie o termináli a užívateľovi poskytované prezenčnými službami[15].....	26
Obrázok 9: PIDF[6].....	27
Obrázok 10: Hlavička metódy SIP PUBLISH [15].....	30
Obrázok 11: Hlavička metódy SIP SUBSCRIBE[15].....	31
Obrázok 12: Proces SUBSCRIBE[15].....	32
Obrázok 13: Hlavička metódy NOTIFY[15].....	32
Obrázok 14: Proces Watcher Information[15].....	33
Obrázok 15: Metóda SUBSCRIBE - presence.wininfo[15].....	33
Obrázok 16: Metóda NOTIFY - presence.wininfo[15].....	34
Obrázok 17: Architektúra Test-bedu.....	41
Obrázok 18: Doba a úsek vyhodnocovania testu.....	43
Obrázok 19: Tok správy PUBLISH sieťou.....	44
Obrázok 20: Cesta k defaultným konfiguračným súborom.....	46
Obrázok 21: Konfiguračné súbory serverov CSCF.....	47
Obrázok 22: Chyby pri spustení P - CSCF	47
Obrázok 23: Spustenie P - CSCF.....	48
Obrázok 24: Spustenie S - CSCF	48
Obrázok 25: Spustenie I - CSCF.....	49
Obrázok 26: Rozhranie Siremis, zoznam watcherov.....	50
Obrázok 27: Moduly serveru v konfiguračnom súbore.....	50
Obrázok 28: Moduly serveru	50
Obrázok 29: Chyba pri spustení serveru.....	51
Obrázok 30: Chyba prezenčného servera Opensips.....	52
Obrázok 31: Boghe IMS/RCS client.....	53
Obrázok 32: Tok správ pri prihlasovaní.....	56
Obrázok 33: Tok správ pri vytváraní relácie.....	57
Obrázok 34: Flow graf, prihlásenie.....	58
Obrázok 35: Čas prihlásenia CPU 0 % RAM 25 % - 75 %	58
Obrázok 36: Čas prihlásenia CPU 100 % RAM 0 % - 75 %	58
Obrázok 37: Priemerná doba prihlásenia CPU 0% RAM 25 % - 75 %.....	59
Obrázok 38: Priemerná doba prihlásenia CPU 100% RAM 0 % - 75 %.....	59
Obrázok 39: Flow graf, IRA.....	61
Obrázok 40: Flow graf, SRD bez presmerovania.....	62
Obrázok 41: SRD bez presmerovania CPU 0 % RAM 25 % - 75 %.....	62
Obrázok 42: SRD bez presmerovania CPU 100 % RAM 0 % - 75 %.....	62
Obrázok 43: Priemerná doba SRD bez presmerovania CPU 0 % RAM 25 % - 75 %....	63
Obrázok 44: Priemerná doba SRD bez presmerovania CPU 100 % RAM 0 % - 75 %..	63
Obrázok 45: Flow graf, ISA.....	65
Obrázok 46: Flow graf, call seetup time.....	65
Obrázok 47: Call setup time CPU 0 % RAM 25 % - 75 %.....	65
Obrázok 48: Call setup time CPU 100 % RAM 0 % - 75 %	66

Obrázok 49: Priemerná doba call setup time CPU 0% RAM 25 % - 75 %.....	66
Obrázok 50: Priemerná doba call setup time CPU 100 % RAM 0 % - 75 %.....	67
Obrázok 51: Flow graf, media delay.....	68
Obrázok 52: Media delay CPU 0 % RAM 25 % - 75 %.....	68
Obrázok 53: Media delay CPU 100 % RAM 0 % - 75 %.....	69
Obrázok 54: Priemerná doba media delay CPU 0 % RAM 25 % - 75 %.....	69
Obrázok 55: Priemerná doba media delay CPU 100 % RAM 0 % - 75 %.....	70
Obrázok 56: Post pick up delay CPU 0 % RAM 25 % - 75 %.....	71
Obrázok 57: Post pick up delay CPU 100 % RAM 0 % - 75 %.....	72
Obrázok 58: Priemerná doba post pick up delay CPU 0 % RAM 25 % - 75 %.....	72
Obrázok 59: Priemerná doba post pick up delay CPU 100 % RAM 0 % - 75 %.....	73
Obrázok 60: Flow graf, ukončenie relácie.....	74
Obrázok 61: Doba ukončenia relácie SDD CPU 0 % RAM 25 % - 75 %	74
Obrázok 62: Doba ukončenia relácie SDD CPU 100 % RAM 0 % - 75 %	75
Obrázok 63: Priemerná doba ukončenia relácie SDD CPU 0 % RAM 25 % - 75 %	75
Obrázok 64: Priemerná doba ukončenia relácie SDD CPU 100 % RAM 0 % - 75 % ...	76

Zoznam tabuliek

Tabuľka1: Parametre testu.....	36
Tabuľka2: Informácie o navrhnutej architektúre IMS siete.....	41
Tabuľka3: Zaznamenané parametre a analýza dát výkonnostného testu.....	42
Tabuľka4: Navrhnutá základňa užívateľov.....	43
Tabuľka5: Priemerná doba prihlásenia CPU 100 % RAM 0 % - 75 %.....	60
Tabuľka6: Priemerná doba prihlásenia CPU 0 % RAM 25 % - 75 %.....	61
Tabuľka 7: Priemerná doba SRD bez presmerovania CPU 100 % RAM 0 % - 75 %....	64
Tabuľka 8: Priemerná doba SRD bez presmerovania CPU 0% RAM 25 % - 75 %.....	64
Tabuľka 9: Priemerná doba call setup time CPU 100 % RAM 0 % - 75 %.....	67
Tabuľka 10: Priemerná doba call setup time CPU 0 % RAM 25 % - 75 %.....	68
Tabuľka 11: Priemerná doba media delay CPU 100 % RAM 0 % - 75 %.....	70
Tabuľka 12: Priemerná doba media delay CPU 0 % RAM 25 % - 75 %.....	71
Tabuľka 13: Priemerná doba post pick up delay CPU 100 % RAM 0 % - 75 %.....	73
Tabuľka 14: Priemerná doba post pick up delay CPU 100 % RAM 0 % - 75 %.....	74
Tabuľka 15: Priemerná doba ukončenia relácie SDD CPU 100 % RAM 0 % - 75 %....	76
Tabuľka 16: Priemerná doba ukončenia relácie SDD CPU 0 % RAM 25 % - 75 %.....	77

Úvod

IP Multimedia Subsystem (IMS) je štandardizovaná Next Generation Network (NGN) architektúra pre telekomunikačných operátorov, ktorý chcú poskytovať multimediálne služby svojim zákazníkom v mobilných aj pevných sieťach. Využíva Voice-over-IP (VoIP) založenú na 3GPP implementácií SIP protokolu a pracuje nad štandardným IP protokolom. Podporuje existujúce telefónne systémy (prepínaných paketov a prepínaných okruhov). Cieľom IMS nie je poskytovať len najnovšie služby, ale všetky služby – tie súčasné aj tie, ktoré bude internet ponúkať v budúcnosti. Mobilným operátorom a poskytovateľom služieb dáva možnosť účtovať každú službu jednotlivo. Navyše dáva možnosť užívateľom využívať ich služby tak v domácej sieti, ako aj v návštevej sieti.

Hlavnou úlohou IMS siete je prepojenie v súčasnosti dvoch najúspešnejších entít v komunikácií a to mobilných sietí a Internetu. Umožňuje koncovým užívateľom využívať mobilné siete pre prístup k internetu a poskytovať tak rôzne multimediálne služby, ktoré Internet ponúka ako prenos dát, videa, audia, telefónnych hovorov a prenosy v reálnom čase, teda poskytuje mobilný Internet. IMS je prístupovo nezávislá, čo znamená, že k nej užívatelia môžu pristupovať z rôznych sietí ako napríklad WLAN (Wireless Local Area Network), ADSL (Asymmetric Digital Subscriber Line) a HFC (Hybrid Fiber-Coaxial).

V prvej kapitole sú opisované funkcionality a požiadavky IMS, ktoré mala naplniť. Druhá kapitola je venovaná protokolom v IMS, protokoly riadenia spojov a AAA protokol. Signalizačný protokol SIP je rozobraný podrobnejšie. Architektúre IMS siete je venovaná tretia kapitola, ktorá je rozdelená do blokov: blok riadenia a smerovania relácií, blok poskytovania služieb zákazníkom, blok medzietrovej komunikácie a databázy. Prezenčná služba je podrobne opísaná v samostatnej štvrtej kapitole. V poslednej piatej kapitole je rozobraný výkonnostný IMS/NGN test podľa špecifikácií TISPAN. Návrh a popis vlastnej architektúry IMS a test – bedu siete založenej na projekte Kamailio, scenáre, ktoré sa budú vykonávať a zaznamenávané parametre výkonnostného testu. V šiestej a siedmej kapitole sa venujem inštalácií a problémom pri inštalácií IMS. Kapitoly 8 a 9 rozoberajú metodiku merania a merané parametre na základe RFC 6076. Posledná desiatka kapitola sú výsledky testov v grafickom prevedení.

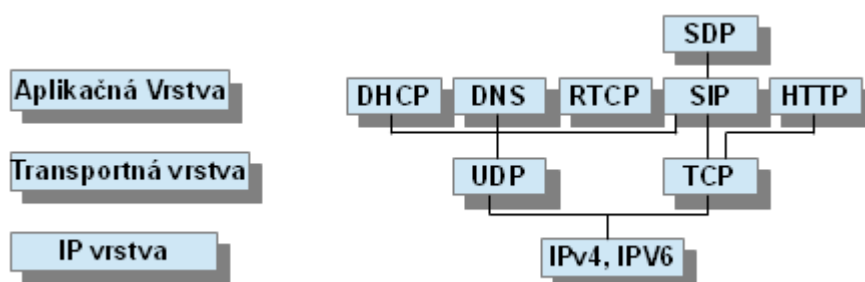
1 Požiadavky na IMS

V návrhu 3GPP (Third Generation Partnership Project) je IMS definovaná ako architektúra vytvorená pre účely poskytnutia IP multimediálnych služieb koncovým zákazníkom. Pri jej vývoji boli kladené požiadavky predovšetkým na zaistenie QoS (Quality of Services) pre služby pracujúce v reálnom čase, nezávislosť prístupu, teda poskytovanie služieb cez IP siete ako GPRS (General packet radio service), WLAN, ADSL, podporu vytvorenia spojenia medzi terminálmi cez SIP protokol, komunikácia medzi Internetom a sieťami prepínaných okruhov a PSTN (Public Switched Telephone Network). Taktiež bola požadovaná možnosť roamingu a schopnosť siete kontrolovať tok dát a s ním súvisiace spoplatnenie poskytovaných služieb. Výrazný vplyv na IMS architektúru mala požiadavka na RCS (Rapid Service Creation). RCS definuje, že IMS služby nemusia byť štandardizované. To znižuje čas za, ktorý je potrebný na uvedenie novej služby do prevádzky.

2 Protokoly v IMS

Protokol je sada pravidiel, ktoré musia byť dodržiavané medzi uzlami siete pri vzájomnej komunikácii [6].

Protokoly SIP (Session Initiation Protocol), SDP (Session Description Protocol) a RTP (Real-time Transport Protocol) sú v IMS využívané aplikačnou vrstvou na popis, riadenie a správu relácií. Na prenos signalizácie sa používajú štandardné transportné protokoly modelu IOS/OSI, TCP (Transmission Control Protocol) a UDP (User datagram protocol) [6].



Obrázok 1: Protokoly v IMS [6]

2.1 Protokoly riadenia spojov

Protokoly, ktoré riadia hovory hrajú kľúčovú úlohu v každom telefónnom systéme, v IMS sú to protokoly založené na IP.

2.1.1 BICC (Bearer Independent Call Control)

Je ďalším vývojom protokolu ISUP (ISDN User Part), BICC na rozdiel od ISUP oddeľuje vrstvu signalizácie od vrstvy médií (audio, video). BICC podporuje rôzne technológie ako IP, SS7 (Signaling System 7), ATM (Asynchronous Transfer Mode) [6].

2.1.2 H.323

Poskytuje vytvorenie multimediálneho spojenia.

2.1.3 SIP (Session Initiation Protocol), RFC 3261

Je signalizačný protokol aplikačnej vrstvy pre vytvorenie a riadenie spojenia v IP sieťach. Je to textovo orientovaný protokol navrhnutý organizáciou IETF (Internet Engineering Task Force). Komunikácia prebieha medzi klientom a serverom formou žiadosť – odpoveď. Protokol bol navrhnutý na základe protokolu SMTP (Simple Mail Transfer Protocol) a HTTP (Hypertext Transfer Protocol).

SIP obsahuje informácie iných protokolov, napríklad použité kódovanie pre multimediálne dáta, čísla portov, na ktorých majú byť dáta prijímané alebo vysielané oddeľuje signalizáciu od dát. Zabezpečuje mobilitu účastníka použitím logickej adresy namiesto fyzickej. Správy protokolu SIP sú tvorené hlavičkou a vlastným telom správy. SIP definuje architektúru skladajúcu sa zo SIP User Agent a SIP serverov. User Agent predstavuje koncové zariadenie siete (softwarové či hardvérové telefóny). V rámci SIP User Agent sa rozlišujú UAC (User Agent Client), ktorý inicializuje spojenie a UAS (User Agent Server), ktorý reaguje na prichádzajúce žiadosti a posielá odpovede na tieto žiadosti. SIP servery umožňujú sprostredkovanie hovorov medzi koncovými účastníkmi [6].

Existujú tri základné druhy SIP serverov:

- *SIP Proxy server* – server analyzuje prichádzajúce správy. Prijíma žiadosti o spojenie od UA alebo iných proxy serverov a preposiela ich ďalšiemu proxy alebo priamo UA.
- *SIP Redirect server* – server priíma žiadosti o spojenie od UA alebo iných proxy serverov a prostredníctvom lokalizačnej služby zistí požadovanú adresu a poskytne ju naspäť klientskému UA.
- *SIP Registrar server* – server prijíma žiadosti o prihlásenie od UA a aktualizuje podľa nich databázu koncových zariadení.

Základná adresa sa nazýva URI (Uniform Resource Identifier), má tvar e-mailovej adresy. *SIP:meno@doména* je príkladom SIP URI. Takýto tvar adresy zvyčajne použije volajúci, ak chce nadviazať spojenie s druhou stranou. Avšak adresa môže obsahovať aj ďalšie

doplňujúce údaje ako napríklad: heslo, port, parametre, hlavičky. Adresa potom vyzerá nasledovne, sip:[užívateľ] [:heslo]@[hostname][:port][parametre][hlavičky] [15].

Žiadosti sú obvykle používané k inicializácii relácie (zostavenie a ukončenie spojenia) alebo oznamujú príjemcovi konkrétnu požiadavku.

- **INVITE** – žiadosť o nadviazanie spojenia alebo o zmenu parametrov existujúceho spojenia
- **BYE** – žiadosť o ukončenie spojenia
- **ACK** – klient potvrdzuje, že obdržal odpoveď na žiadosť INVITE
- **REGISTER** – žiadosť o registráciu klienta na registrar server
- **CANCEL** – žiadosť o zrušenie prebiehajúcej žiadosti INVITE
- **OPTIONS** – žiadosť o zaslanie podporovaných funkcií na servery
- **INFO** – prenos informácií behom hovoru

Odpovede sú trojmiestne kódy označujúce výsledok žiadosti, dajú sa identifikovať podľa prvej číslice.

- **1xx** (informačná) – požiadavka bola prijatá a spracováva sa
- **2xx** (úspech) – činnosť bola úspešne realizovaná
- **3xx** (presmerovanie) – musia byť vykonané ďalšie procedúry pre realizovanie požiadavky
- **4xx** (chyba klienta) – chyba na strane klienta
- **5xx** (chyba serveru) – server zlyhal pri spracovaní požiadavky
- **6xx** (všeobecná porucha) – požiadavka nebude vykonaná ani na inom servery

Ďalšie dve číslice sú pre každú triedu presne definované a vyjadrujú konkrétne stavy v danej triede.

To, že protokol SIP je založený na protokole HTTP umožňuje vývojárom využívať všetky štruktúry vyvinuté pre HTTP, čo zjednodušuje a urýchľuje tvorbu nových služieb. Táto skutočnosť mala veľký vplyv na výber protokolu SIP ako protokolu riadenia relácií v IMS [6][15].

2.1.4 RTP (Real-time Transport Protocol)

Tento protokol umožňuje prenášať dáta v reálnom čase ako video, audio cez nespoľahlivo orientované spojenie (UDP). Avšak protokol sám osebe dáta neprenáša, zabezpečuje ich rekonštrukciu na strane príjemcu pomocou časových známk. Vždy sa používa spoločne s protokolom RTCP (RTP Control Protocol), ktorý poskytuje QoS štatistiky [6][15].

2.1.5 SDP (Session Description protocol)

SDP je textovo orientovaný protokol a slúži na popis relácie, ktorá bude vytvorená medzi terminálmi.

Popis obsahuje potrebné informácie pre užívateľa, aby sa mohol pripojiť k relácii. Informácie obsahujú IP adresu a číslo portu, kam budú dáta odosielané a použité kodeky.

SDP popis sa skladá z dvoch častí, popis relácie a popis prenášaných dát. Príklad SDP popisu je na obrázku (Obr.č.2). Prvých päť riadkov je popis relácie, obsahujú verziu a identifikátory užívateľa (v,o-riadky), predmet relácie (s-riadok), IP adresa odosielateľa (c-riadok), čas relácie (t-riadok). Riadky a a m popisujú prenášané dáta. V tomto prípade audio, číslo portu a kodeky, a-riadok značí príjem aj odosielanie dát.

```
V=1
o=Martin 2787498654 2867892807 IN IP4 192.168.1.3
s=sflphone
c=IN IP4 192.168.1.3
t=2 0
m=audio 20000 RTP/AVP 0
a=sendrecv
m=video 20002 RTP/AVP 31
a=sendrec
```

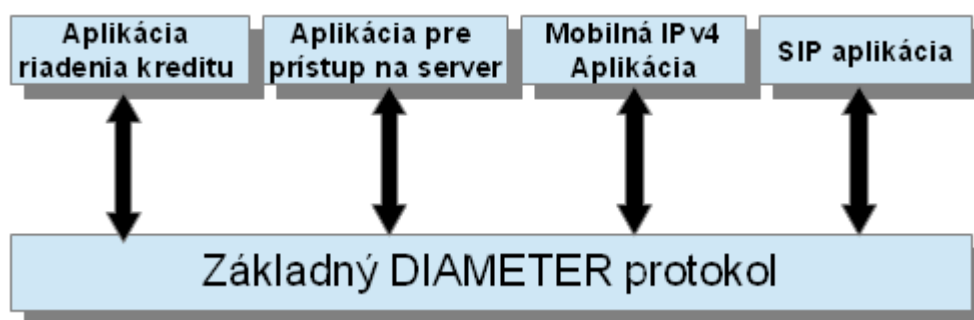
Obrázok 2: SDP [6]

2.2 AAA protokol

AAA (Authentication, Authorization, and Accounting) protokol zabezpečuje autentifikáciu, autorizáciu a správu účtov. V IMS bol zvolený ako AAA protokol DIAMETER protokol. Je pokračovaním protokolu RADIUS [6].

2.2.1 DIAMETER

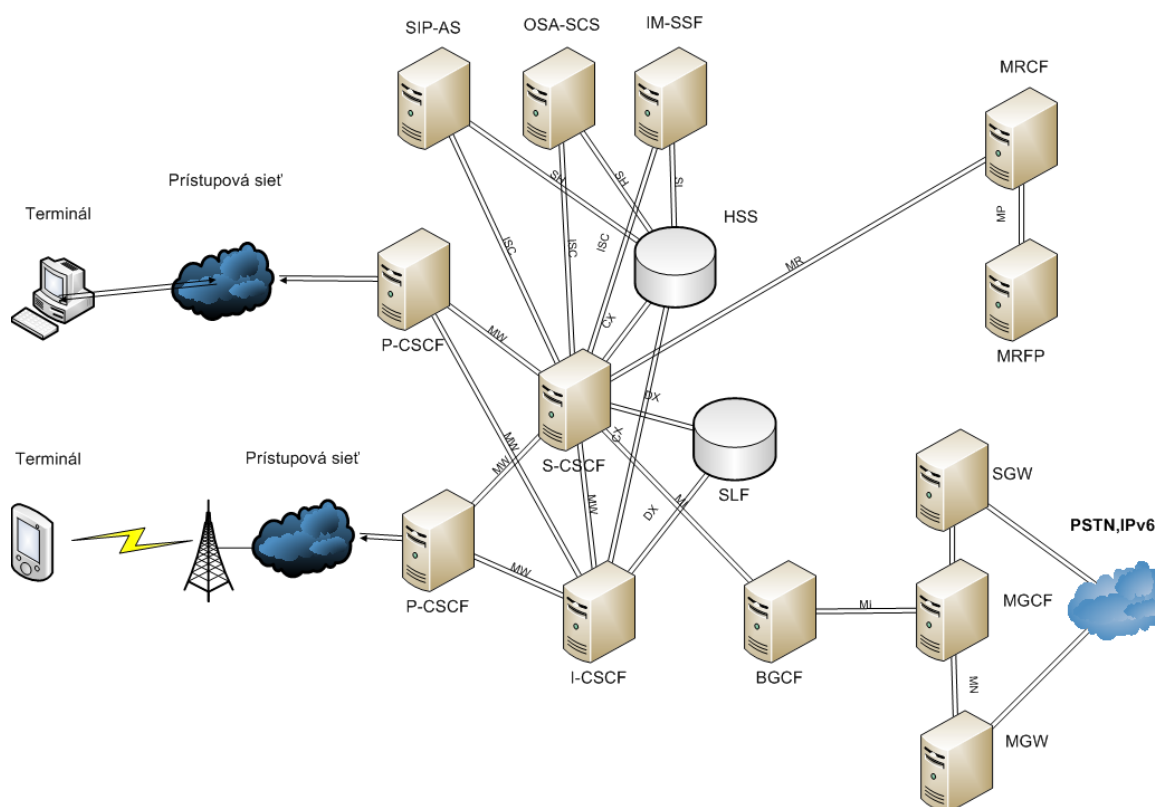
DIAMETER protokol bol vyvinutý ako základný protokol a aplikácie, ktoré dopĺňajú základnú funkciu protokolu. Základní protokol zabezpečuje riešenie chýb, doručovanie dátových jednotiek a poskytovanie rozširiteľnosti formou nových aplikácií. Aplikácie sú využívané pri konkrétnom využití protokolu.(Obr.3) [6][15].



Obrázok 3: Vzťah medzi základným protokolom a jeho aplikáciami[6]

Protokol využíva pri komunikácii rôzne druhy správ [6].

- ACR – (Accounting Request)
- ACA – (Accounting Answer)
- CER – (Capabilities Exchange Request)
- CEA – (Capabilities Exchange Answer)
- CCR – (Credit Control Request)
- CCA – (Credit Control Answer)
- DWR – (Device Watchdog Request)
- DWA – (Device Watchdog Answer)
- RAR – (Re Auth Request)
- RAA – (Re Auth Answer)[6]



Obrázok 4: Architektúra IMS

3 Architektúra IMS

Architektúra IMS má tri vrstvy: Transportná vrstva, IMS vrstva (Control/Signaling Plane) a Aplikačná vrstva [5].

3.1 Blok riadenia a smerovania relácií

Táto funkcia hrá dôležitú úlohu počas vytvárania relácie a prihlásenia, taktiež zaisťujú v IMS sieti smerovanie signalizácie a generujú dáta pre vyúčtovanie.

Uzly, ktoré v IMS vykonávajú túto úlohu sú CSCF (Call Session Control Function), sú to SIP servery, ktoré spracovávajú signalizáciu, zúčastňujú sa prihlasovania, vytvárania relácií a vytvárajú smerovací aparát v IMS. Existujú štyri druhy CSCF v závislosti na ich funkcionalite, P-CSCF (Proxy), S-CSCF (Serving), I-CSCF (Interrogating). V 3GPP vydaní 7 je špecifikovaný server E-CSCF (Emergency) [17].

3.1.1 P-CSCF (Proxy Call Session Control Function)

Je to prvý kontaktný bod pre užívateľov v rámci IMS, to znamená že všetka SIP signalizácia z terminálov bude posielaná P-CSCF. Podobne aj všetka končiaca SIP signalizácia smerujúca zo siete je posielaná P-CSCF. P-CSCF smeruje SIP odpovede a žiadosti do príslušnej destinácie, IMS terminálu alebo IMS siete. Pri registrácii je pridelený IMS terminálu jeden P-CSCF a ten

sa v priebehu prihlasovania nemení, terminál komunikuje len z jedným P-CSCF. P-CSCF vytvára IPsec spojenie s IMS terminálom, toto spojenie zabezpečuje integritu dát, teda schopnosť kontrolovať obsah správy – či bol zmenený alebo nie. Autentifikácia užívateľa prebieha počas naväzovania IPsec spojenia. Ak P-CSCF autentifikuje užívateľa potvrdzuje identitu užívateľa všetkým uzlom v sieti, tie tak nemusia užívateľa znovu autentifikovať. P-CSCF overuje správnosť SIP žiadostí, ktoré zasiela terminál, zabráňuje sa tak vytváraniu žiadostí, ktoré nie sú podľa SIP pravidiel.

Ďalšou funkciou P-CSCF je kompresia a dekompresia SIP správ na rozhraní medzi terminálom a IMS sieťou. Veľké správy môžu byť cez prístupové siete prenášané niekoľko sekúnd, preto na zníženie času prenosu sa využíva kompresia, P-CSCF vykoná kompresiu a terminál na druhej strane dekompresiu a naopak. P-CSCF taktiež generuje informácie pre vyúčtovanie a udržiava časovače spojenia

IMS sieť obsahuje niekoľko P-CSCF pre zaistenie rozšíriteľnosti a spoľahlivosti. Každý P-CSCF obsluhuje niekoľko IMS terminálov v závislosti na kapacite uzla [17][6].

3.1.2 I-CSCF (Interrogating Call Session Control Function)

I-CSCF je kontaktný bod v rámci operátorovej siete pre všetky spojenia určené užívateľom operátorovej siete. Pri prihlásení užívateľa získa meno ďalšieho skoku (S-CSCF) z HSS (Home Subscriber Server) a následne vykonáva smerovanie SIP žiadostí a odpovedí do zvoleného S-CSCF. Dodatočne I-CSCF môže voliteľne šifrovať časti SIP správ, ktoré obsahujú citlivé informácie o doméne, ako počet serverov v doméne, ich DNS mená alebo ich kapacitu. Táto funkcia sa označuje ako THIG (Topology Hiding Inter-network Gateway).

Pre zaistenie rozšíriteľnosti a spoľahlivosti IMS obsahuje niekoľko I-CSCF [17][6].

3.1.3 S-CSCF (Serving Call Session Control Function)

S-CSCF je hlavným uzlom v IMS, ktorý je zodpovedný za spracovanie prihlasovacieho procesu, smerovacích rozhodnutí a udržiavanie relácií. Ak užívateľ zašle žiadosť o prihlásenie, táto žiadosť bude smerovaná na S-CSCF, ktorý stiahne autentifikačné dáta z HSS. Po získaní dát z HSS generuje výzvu terminálu k autentifikácii, po obdržaní a overení odpovede s terminálu S-CSCF prijme prihlásenie. Po tejto procedúre je užívateľ schopný využívať IMS služby. S-CSCF pri prihlásení stiahne tzv. service profile s HSS a doručí ho užívateľovi [17][6].

Service profile je súhrn informácií o užívateľovi, ktorý je permanentne uložený v HSS a priradený k verejnej identite užívateľa (napr. peter@example.com). Na základe informácií v service profile, S-CSCF sa rozhodne, ktorý aplikačný server kontaktuje, keď užívateľ pošle SIP žiadosť alebo prijme žiadosť. Service profile môže obsahovať zoznam služieb, ktoré má

užívateľ dovolené využívať, napr. len audio. To súvisí s ďalšou úlohou S-CSCF a tou je výkon politiky operátora, zabráňuje užívateľom pristupovať k nepovoleným službám.

Jedna z hlavných úloh S-CSCF je poskytovať SIP smerovacie služby, ak obdrží žiadosť z terminálu cez P-CSCF je nutné rozhodnúť či bude kontaktovaný aplikačný server skôr ako bude požiadavka odoslaná ďalej. Ak je kontaktovaný aplikačný server relácia pokračuje v rámci IMS alebo pokračuje v inej doméne (v inej IP sieti). Pred odoslaním požiadavky na P-CSCF, S-CSCF môže smerovať žiadosť na aplikačné servery pre potreby kontroly presmerovacích inštrukcií.

S-CSCF slúži aj ako prekladač medzi telefónnymi číslami a SIP URI, ak užívateľ vytočí telefónne číslo namiesto SIP URI, tak S-CSCF vykoná preklad založený na DNS E.164 Number Translation.

V sieti sa zvyčajne nachádza niekoľko S-CSCF za účelom zaistenia rozšíriteľnosti a spoľahlivosti, každý S-CSCF obsluhuje niekoľko IMS terminálov, v závislosti na kapacite uzla [17][6].

3.1.4 E-CSCF (Emergency Call Session Control Function)

E-CSCF je entita, ktorá spracováva naliehavé a krízové žiadosti, ako napríklad volania na políciu, hasičský zbor a zdravotnú pomoc. Jeho hlavnou úlohou je vybrať server pre núdzové prípady, tiež známy ako Public Safety Answering Point, kam má byť doručená núdzová žiadosť [17][6].

3.2 Blok Služieb poskytovaných užívateľom

Služby poskytované užívateľom v IMS sú zabezpečované aplikačnými servermi a MRF (Media Resource Function). V sieti zvyčajne býva niekoľko aplikačných serverov, každý je špecializovaný na poskytovanie určitej služby. Servery implementujú technológie ako Java, SIP servlets, alebo SIP CGI (Common Gateway Interface) atď. Každý aplikačný server priamo komunikuje s S-CSCF. Prepojenie medzi aplikačnými servermi a S-CSCF je realizované pomocou IMS Service Control (ISC).

Šieste vydanie 3GPP definuje rozhranie pre prepojenie aplikačných serverov a terminálov Ut, je využívané užívateľmi, napríklad pre správu a manažovanie politik, nepoužíva sa pre prenos multimediálnych dát. Protokol využívaný Ut je založený na XCAP (XML Configuration Access Protocol). XCAP definuje ako používať HTTP na vytváranie, úpravu a mazanie XML dokumentov.

V rámci IMS sú definované tri typy aplikačných serverov závislosti na ich funkcionalite, SIP AS, OSA-SCS (Open Service Access-Service Capability Server) a IM-SSF (IP Multimedia Service Switching Function) [2][6].

3.2.1 SIP aplikačný server

Je to natívny aplikačný server v IMS, slúži ako úložisko a spúšťa služby užívateľov ako prezenciu, posielanie textových správ a multimediálnu telefóniu. Tento server sa spája s HSS rozhraním Sh, avšak len v domácej sieti, Sh využíva protokol DIAMETER a rozhraním Ut sa spája s terminálom [6][15].

3.2.2 OSA-SCS (Open Service Access-Service Capability Server)

Umožňuje spúšťanie OSA služieb v IMS sieti. Väčšina služieb pre IMS bola navrhnutá pre SIP aplikačné servery, avšak stále existujú služby navrhnuté pre OSA aplikačné servery. Takže OSA-SCS zaisťuje prístup k týmto službám s IMS.

OSA-SCS poskytuje spojenie k OSA aplikačnému serveru, dokáže pristupovať do IMS bezpečne z externých sietí. Na jednej strane komunikuje s S-CSCF a HSS pomocou SIP a na druhej strane komunikuje s OSA aplikačným serverom a OSA aplikačným programovacím rozhraním [2][6].

3.2.3 IM-SSF (IP Multimedia Service Switching Function)

Tento server dovoľuje užívateľom používať CAMEL (Customized Applications for Mobile network Enhanced Logic) služby používané v GSM (*Global System for Mobile Communications*) sieťach, predstavuje bránu medzi SIP a CAMEL službami. Taktiež IM-SSF umožňuje GSMSCF (GSM Service Control Function) kontrolovať IMS reláciu. Ako aplikačný server sa spája s S-CSCF a HSS na jednej strane a na druhej strane vystupuje ako SSF (Service Switching Function) spájajúc sa s GSMSCF (GSM Service Control Function), protokolom založenom na CAP (CAMEL Application Part).

Z pohľadu protokolu SIP, aplikačné servery môžu vystupovať ako SIP User Agent, SIP Proxy a SIP B2BUA.

3.2.4 Aplikačný server ako SIP User Agent

Ak je destinácia relácie určená ako aplikačný server, potom tento server vystupuje ako User Agent, poskytuje služby volajúcemu. To platí aj v opačnom prípade, kedy server vystupuje ako volajúci. Príklad takejto situácie nastane, keď server inicializuje reláciu smerom k terminálu a vykoná tzv. wake-up call service.

3.2.5 Aplikačný server ako SIP Proxy Server

Aplikačný server vystupuje ako proxy vtedy, ak žiadosť odoslaná z terminálu do P-CSCF a následne na S-CSCF je týmto S-CSCF presmerovaná na aplikačný server a ten žiadosť ďalej prepošle na ďalší S-CSCF server. S-CSCF v tomto prípade pridá do hlavičky žiadosti tzv. SIP hlavičku Route. Toto pole umožňuje aplikačnému

serveru prijatú žiadosť odoslať späť na S-CSCF, ktoré odošle žiadosť ďalej. Pri tomto úkone S-CSCF vloží do SIP hlavičky Route informácie o vlastnom SIP URI, to mu umožňuje rozpoznať či prijatá žiadosť bola už prijatá od terminálu a odoslaná na aplikačný server. Príklad SIP hlavičky Route (Obr.č.5).

Route: <sip:as33.home1.net;lr>, <sip:state34@scscf1.home1.net;lr>

Obrázok 5: Route field [6]

Hlavička sa skladá z dvoch SIP URI, prvá určuje aplikačný server a druhá adresa odkazuje na S-CSCF (hlavička môže obsahovať viac ako dve SIP URI). Avšak S-CSCF vloží Route field do žiadosti vždy, či server vystupuje ako SIP UA alebo SIP Proxy.

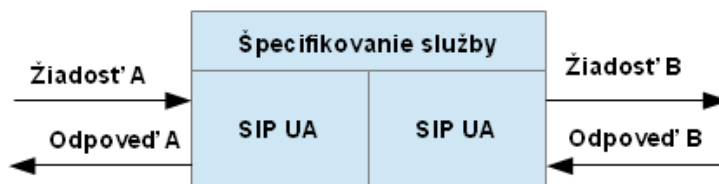
3.2.6 Aplikačný server ako SIP Redirect Server

Táto situácia nastane ak S-CSCF presmeruje prijatú žiadosť na aplikačný server a ten odpovedá správou 302 Moved Temporarily, ktorá je odoslaná naspäť terminálu. Hlavička správy obsahuje Contact field, v ktorom sa nachádza nová URI adresa, na ktorú terminál odošle novú žiadosť INVITE.

Typický príklad použitia SIP redirect serverov je v prípade využitia služby presmerovanie hovorov [6].

3.2.7 Aplikačný server ako SIP B2BUA

B2BUA je v podstate spojenie dvoch SIP UA pomocou Service-specific logic (Obr.č.6). Vykonáva podobné akcie ako SIP Proxy, prijíma žiadosti, odpovede a presmerováva ich ďalej [6].



Obrázok 6: SIP B2B UA[6]

Existujú tri druhy aplikačných serverov a každý komunikuje s S-CSCF a HSS. Cez SIP komunikujú s S-CSCF a protokolom DIAMETER sa spájajú s HSS, kam nahrávajú alebo sťahujú informácie týkajúce sa užívateľov.

3.2.8 MRF (Media Resource Function)

MRF poskytuje transkódovanie medzi odlišnými kodekmi, kombinovanie tokov dát od rôznych užívateľov pre vytvorenie konferenčného hovoru, získava štatistiky a vykonáva analýzu dát, delí sa na dve časti: MRFC (Media Resource Function Controller) a MRFP (Media Resource Function Controller) [6].

3.2.9 MRFC (Media Resource Function Controller)

MRFC vystupuje ako SIP User Agent a komunikuje s S-CSCF cez SIP, riadi zdroje v MRFP, s ktorým komunikuje cez H.248/MEGACO protokol [6].

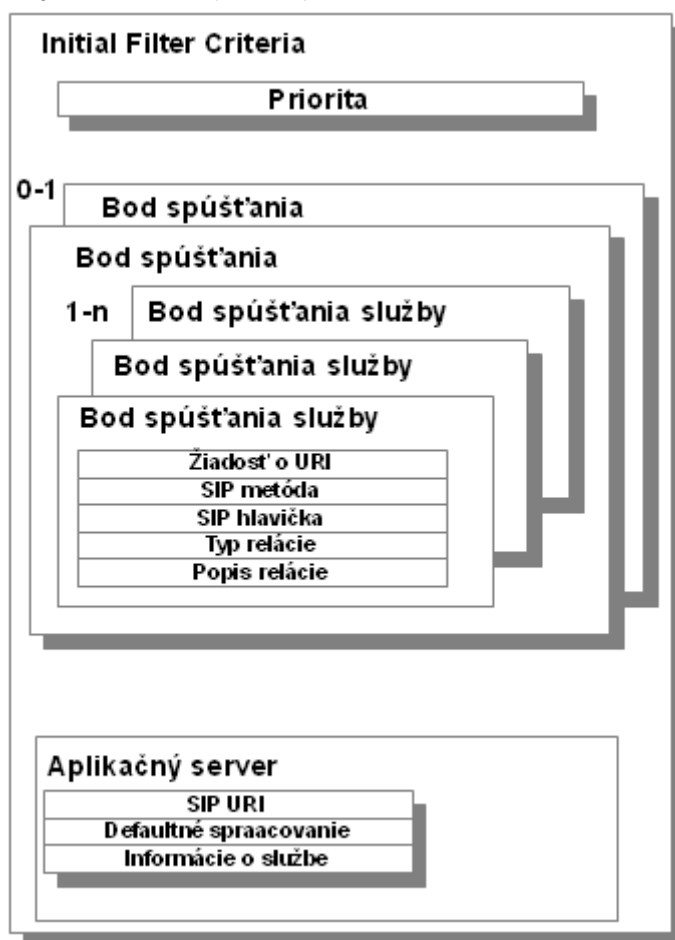
3.2.10 MRFP (Media Resource Function Controller)

V rámci IMS je MRFP využité pri konferenčných hovoroch, kedy zmiešava jednotlivé dátové toky a odosiela takto kombinované dáta všetkým zúčastneným.

Ak jednotliví účastníci konferenčného hovoru používajú odlišné audio alebo video kodeky MRFP vykoná preklad do kodekov jednotlivých účastníkov hovoru [6].

3.2.11 Initial Filter Criteria

Initial filter criteria definujú, ako sa bude zaobchádzať so SIP správami prijatými S – CSCF, presnejšie na ktorý aplikačný server má S – CSCF odoslať prijatú žiadosť, aby bola užívateľovi poskytnutá požadovaná služba. Ak S – CSCF prijme SIP požiadavku, stiahne IF kritériá z HSS, ktoré sú súčasťou profilu užívateľa a podľa nich odošle žiadosť na príslušný aplikačný server. IF kritériá sú v podstate profily služieb, sú kódované v XML (Extensible Markup Language) kóde. Štruktúra IF kritérií je na obrázku (Obr.č.7) [4].



Obrázok 7: Initial Filter Criteria[6]

- Priority – hodnota, ktorá určuje v akom poradí sa budú vyhodnocovať IF kritériá, ktoré sú súčasťou rovnakého profilu služby, priorita 1 je najvyššia a spracováva sa ako prvá.
- Trigger point – informácia o tom, či bude žiadosť odoslaná na aplikačný server alebo nie, skladá sa z Service Point Triggers, ak IF kritérium neobsahuje trigger point žiadosť, je automaticky odoslaná na aplikačný server. Request-URI určuje adresu prijímateľa žiadosti. SIP Method určuje typ žiadosti (INVITE alebo MESSAGE). SIP Header obsahuje informácie o samotnej žiadosti. Session Case môže nadobúdať hodnoty, Originating, Terminating, Originating_Unregistered alebo Terminating_Unregistered.
- Application Server – obsahuje informácie týkajúce sa aplikačného servera, na ktorý má byť požiadavka odoslaná. SIP URI je adresa aplikačného servera, Default Handling definuje čo sa má vykonať, ak sa S – CSCF nedokáže spojiť s aplikačným serverom. Service Information Field obsahuje dáta, ktoré môžu byť potrebné pri spracovaní žiadosti aplikačným serverom.

IF kritériá sú využívané, keď S – CSCF obdrží SUBSCRIBE, INVITE alebo OPTION. Pri obdržaní PRACK, NOTIFY, UPDATE alebo BYE, IF kritériá nie sú použité [1][6].

3.3 Databázy

V IMS sú dve hlavné databázy: HSS (Home Subscriber Server) a SLF (Subscription Locator Function).

HSS slúži ako hlavné úložisko dát všetkých užívateľov a dát týkajúcich sa služieb IMS.

3.3.1 Databázy HSS a SLF

Home Subscriber Server je centrálné úložisko pre informácie týkajúce sa užívateľov. HSS obsahuje informácie o profile užívateľa, aké služby využíva, ktorý S-CSCF server je pridelený konkrétnemu užívateľovi, bezpečnostné informácie (autentifikačné a autorizačné dáta). Pri registrácii do HSS pristúpi S-CSCF a stiahne si profil užívateľa. HSS obsahuje HLR (Home Location Register), ktorý umožňuje spoluprácu s uzlami sietí prepínaných okruhov, vďaka čomu môže užívateľ pristupovať do týchto sietí.

V sieti môže byť viacero HSS v závislosti od počtu užívateľov. Sieť s viacerými HSS vyžaduje SLF. SLF je databáza, ktorá obsahuje záznam o tom v ktorej HSS databáze sa nachádza užívateľ, čiže ak sa nejaký uzol dotazuje SLF s adresou užívateľa ako odpoveď dostane adresu HSS, ktorá obsahuje informácie o danom užívateľovi [6][15].

3.4 Služby zabezpečujúce medzi-sieťovú komunikáciu

Pri vzájomnej komunikácii medzi užívateľmi sa vyskytne prípad, kedy jeden komunikuje s IPv4 sieťou alebo IPv6 sieťou do sietí prepínaných okruhov ako PLMN (Public Land Mobile Network) alebo PSTN. Vtedy je nutné zabezpečiť komunikáciu medzi odlišnými komunikačnými protokolmi. Túto funkciu vykonávajú prvky BGCF, IMS-ALG, TrGW, SGW, MGW a MGCF [6].

3.4.1 BGCF (Breakout Gateway Control Function)

V podstate je to SIP server, ktorý vykonáva smerovanie založené na telefónnych číslach. BGCF sa využije v prípade relácie určenej účastníkovi v sieti prepínaných okruhov, ako napríklad PSTN alebo PLMN.

Jeho hlavnou úlohou je výber PSTN/CS brány pre prepojenie IMS s PSTN [6][15].

3.4.2 IMS-ALG (Application Layer Gateway) a TrGW (Translation Gateway)

IMS podporuje oba IP protokoly Ipv4 aj Ipv6, aby bola zaistená bezproblémová komunikácia pri použití rozdielnych verzií IP protokolu bez nutnosti podpory oboch protokolov terminálmi, IMS pridalo do svojej architektúry dva prvky, ktoré vykonávajú preklad medzi týmito protokolmi.

IMS-ALG pôsobí ako SIP B2BUA vytvorením dvoch nezávislých spojení s vnútornou IMS

(IPv4) sieťou a vonkajšou sieťou, ktorej IP protokol je odlišnej verzie (IPv6). IMS-ALG prepíše SDP relácie inicializovanej terminálom a to konkrétne IP adresu a čísla portov za IP adresu a porty priradené TrGW, táto operácia umožňuje, aby mohli byť dáta smerované do TrGW.

TrGW je v podstate NAT-PT/NAPT-PT (Network Address Port Translator-Protocol Translator). Obsahuje pool IPv4 adries, ktoré sú dynamicky priradované jednotlivým reláciám [6].

3.4.3 SGW (Signaling Gateway)

Úlohou SGW je preklad signalizácie na transportnej vrstve medzi signalizáciou založenej na IP a signalizácie založenej na SCTP/IP a SS7 [6].

3.4.4 MGCF (Media Gateway Control Function)

Zabezpečuje prepojenie medzi sieťou prepínaných paketov a sieťou prepínaných okruhov. Hovory, ktoré sú uskutočňované zo siete prepínaných okruhov (PSTN), sú smerované na tento uzol na aplikačnej vrstve vykoná preklad správ BICC/ISUP na SIP správy a odošle ich na P-CSCF [6][15].

3.4.5 MGW (Media Gateway)

Spája IMS s dátovou vrstvou PSTN siete, prijíma dáta z IMS cez RTP protokol a spája sa s PSTN sieťou využívaním PCM (Pulse Code Modulation) časových slotov. Dodatočne vykonáva preklad, ak IMS terminál nepodporuje kodeky používané PSTN sieťou [6][15].

4 Prezenčné služby

Prezenčné služby poskytujú užívateľom informácie o dostupnosti a možnosti komunikácie s inými užívateľmi. Prezenčná služba je schopná poskytnúť informácie, či sú iní užívatelia online alebo nie a ak sú online, či sú obsadený alebo môžu prijať hovor. Navyše prezenčné služby užívateľom poskytnú detailné informácie o ich komunikačných prostriedkoch a možnostiach (Obr.č.8).



Obrázok 8: Informácie o termináli a užívateľovi poskytované prezenčnými službami[15]

V rámci procedúr prezenčných služieb sú definované rôzne úlohy, užívateľ alebo terminál, ktorý práve poskytuje prezenčné informácie prezenčným službám je nazývaný *prezenčná entita*, ktorá prostredníctvom PUA (Presence User Agent) implementovaným v IMS termináli (počítač, mobilný telefón) poskytuje informácie o svojom charaktere. PUA následne preposiela informácie do PA (Presence Agent), ktorý je súčasťou PS (Presence Server). Prezenčný server vykonáva funkcie PA, ako aj proxy server pre žiadosti SUBSCRIBE.

Ďalšou úlohou v rámci prezenčných služieb je tzv. watcher. Watcher je prvok, ktorý práve žiada od PA prezenčné informácie od prezenčnej entity alebo o svojich watcheroch.

Ako signalizačný protokol v 3GPP (3rd Generation Partnership Project) IMS bol zvolený SIP, preto 3GPP tiež prijal rozšírenie SIP protokolu navrhnuté IETF SIMPLE (SIP for Instant Messaging and Presence Leveraging Extensions) ako signalizačný protokol pre IMPS (Instant Messaging and Presence Service). V tomto SIP rozšírení sa metóda SIP MESSAGE používa pre doručenie okamžitých správ (instant messages) a metódy PUBLISH, SUBSCRIBE a NOTIFY sú využívané prezenčnými službami (presence services) [6][15].

4.1 Prezenčné informácie – formát dát

Prezenčné informácie sú prenášané vo formáte PIDF (Presence Information Data Format), ktorý je nezávislý na protokole, teda aj iný protokol ako SIP môže byť použitý na prenos prezenčných informácií medzi dvoma prezenčnými entitami. Je minimalisticky navrhnutý za účelom splnenia základných požiadaviek, čo zaručuje kompatibilitu s inými protokolmi. Taktiež je dobre rozšíriteľný, ak je potrebné viac ako umožňuje základný model.

PIDF kóduje prezenčné informácie v XML dokumente, ktorý môže byť prenesený ako hociktorý iný MIME dokument.

PIDF definuje nový typ média `application/pidf+xml` [2], ktorý indikuje typ aplikácie a kódovania. Dokument obsahuje prezenčné informácie ako online (open), offline (closed), kontakt, časovú známku a iné podľa verzie PIDF. Príklad PIDF je na obrázku (Obr.č.9) [2][6].

```
<?xml version="1.0" encoding="UTF-8"?>
<presence xmlns="urn:ietf:params:xml:ns:pidf"
  entity="pres:alice@example.com">

  <tuple id="qoica32">
    <status>
      <basic>open</basic>
    </status>
    <contact priority="0.9">tel:+1555876543</contact>
    <note>My cell phone</note>
  </tuple>
</presence>
```

Obrázok 9: PIDF[6]

4.2 Prezenčné služby v IMS

Prezenčná služba bola pôvodne uvedená v 3GPP vydaní 6, avšak neskôr OMA (Open Mobile Alliance) prevzala prezenčné služby založené na IMS a v súčasnosti je OMA najkomplexnejšia organizácia zaoberajúca sa prezenčnými službami. V OMA Presence architecture sú definované nasledujúce prvky [16][1].

4.2.1 Presence server

IMS aplikačný server, ktorý manažuje prezenčné informácie získané z prezenčných zdrojov a spravuje prezenčné žiadosti o prístup na server [16].

4.2.2 Resource List Server

Aplikačný server, ktorý prijíma a manažuje žiadosti o prezenčný zoznam, ktorý umožňuje watcher aplikáciám získať prezenčné informácie viacerých prezenčných entít za použitia jednej transakcie [16][15].

4.2.3 XDMS (XML Document Managemet Servers)

Aplikačné servery, ktoré uchovávajú informácie týkajúce sa prezenčných služieb vo formáte XML dokumentov. Označovaný aj ako XCAP server. Sú definované štyri typy serverov:

- Presence XDMS – server, ktorý obsahuje pravidlá pre žiadosť o získanie prezenčných informácií, pravidlá pre publikovanie prezenčných informácií
- RLS XDMS – server, ktorý obsahuje buddylist-y jednotlivých užívateľov. Buddylist je zoznam, ktorý umožňuje vidieť napríklad kto je online alebo offline.
- Presence Content XDMS – server, ktorý spravuje informácie týkajúce sa prenášaných dát
- Shared XDMS – server, ktorý môže byť v prípade nutnosti použitý inými aplikačnými servermi

V praxi sú tieto typy serverov realizované pomocou jedného XDMS servera, ktorý v sebe zahŕňa všetky funkcionality [16][15].

4.2.4 XCAP (XML Confiduration Access Protocol)

Protokol XCAP definovaný organizáciou IETF bol zvolený OMA a 3GPP ako protokol pre prenos, prístup, čítanie a manipuláciu XML dokumentov z XDMS serveru. Umožňuje užívateľom nahráť dáta na XCAP server, ktorý tieto informácie poskytuje iným aplikačným serverom a tie sú na základe týchto informácií schopné poskytnúť požadované služby užívateľom. XCAP používa HTTP protokol na nahrávanie a čítanie informácií z XCAP serveru [15].

4.2.5 Content server

Je schopný manažovať MIME (Multipurpose Internet Mail Extensions) objekty, dovoľuje prezenčným zdrojom alebo prezenčnému serveru ukladať MIME objekty [15].

4.2.6 Presence source

Entita, ktorá poskytuje prezenčné informácie prezenčným službám [15].

4.2.7 Presence watcher

Entita, ktorá žiada o informácie o prezenčných entitách [15].

4.2.8 Watcher agent

Spravuje watcher-ve prezenčné služby v jeho doméne [15].

4.3 Zverejnenie prezenčných informácií

Pri zverejnení alebo aktualizácii prezenčných informácií, terminál uploaduje tieto informácie použitím metódy SIP PUBLISH na prezenčný server (Obr.č.10)

```
PUBLISH sip:presentity@example.com SIP/2.0
To: <sip:presentity@example.com>
From: <sip:presentity@example.com>;tag=1234wxyz
Expires: 3600
Event: presence
Content-Type: application/pidf+xml
...

<?xml version="1.0" encoding="UTF-8"?>
<presence xmlns="urn:ietf:params:xml:ns:pidf"
  xmlns:op="urn:oma:xml:prs:pidf:oma-pres"
  entity="sip:presentity@example.com@example.com">
  <tuple id="a1232">
    <status>
      <basic>open</basic>
    </status>
    <op:willingness>
      <op:basic>open</op:basic>
    </op:willingness>
    <op:registration-state>active</op:registration-state>
    <op:service-description>
      <op:service-id>org.openmobilealliance:
        PoC-session</op:service-id>
      <op:version>1.0</op:version>
    </op:service-description>
    <contact>sip:presentity@example.com@example.com</contact>
    <timestamp>2008-05-26T12:00:00Z</timestamp>
  </tuple>
</presence>
```

Obrázok 10: Hlavička metódy SIP PUBLISH [15]

- PUBLISH sip – koho prezenčné informácie budú zverejnené
- Expires – ako dlho budú informácie validné
- Event – identifikuje typ žiadosti na prezenciu, podľa ktorej S-CSCF presmeruje túto žiadosť na prezenčný server

Ďalšia časť žiadosti obsahuje aktuálne prezenčné informácie v XML kóde a to, že užívateľ je registrovaný, k dispozícii, schopný komunikácie, dostupná služba je Push to talk Over Cellular [15].

4.4 Získanie prezenčných informácií

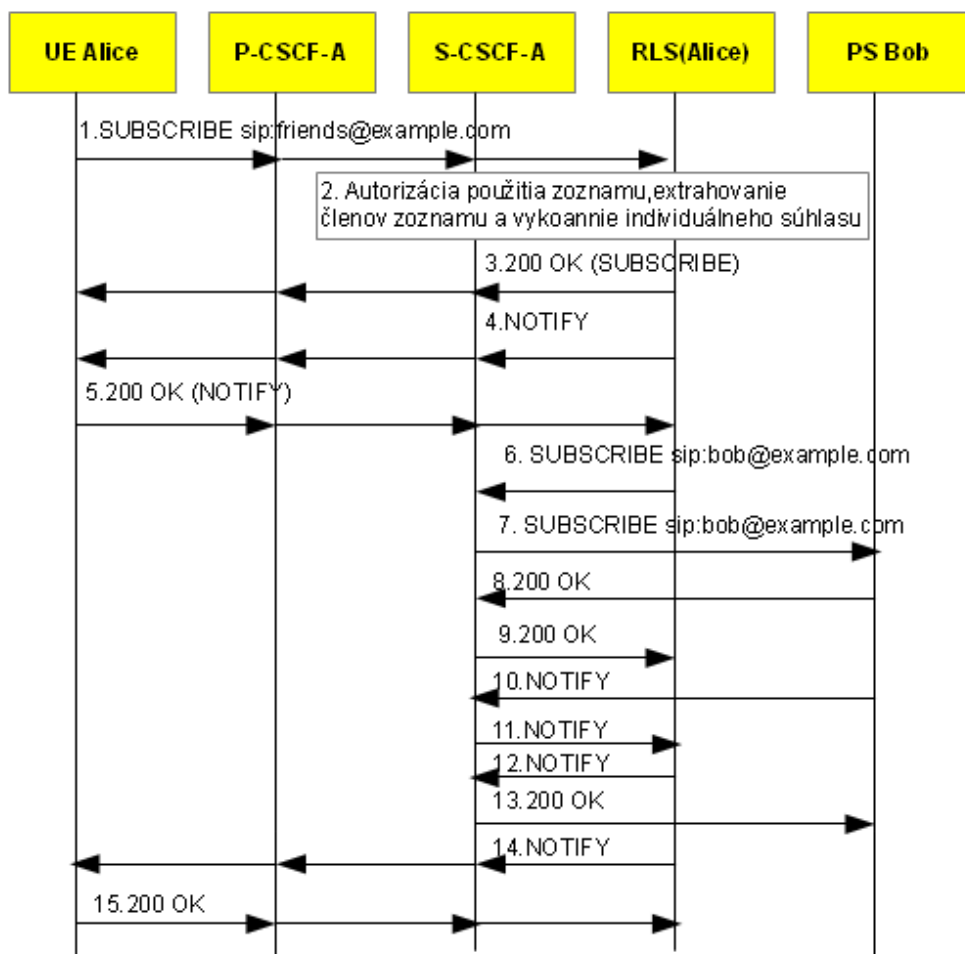
Ak watcher chce získať prezenčné informácie o iných užívateľoch musí vytvoriť SIP SUBSCRIBE žiadosť, určenú pre konkrétnu prezenčnú entitu alebo pre watcherov vlastný prezenčný zoznam užívateľov (presence list), o ktorých chce získať prezenčné informácie.

```
SUBSCRIBE sip:friends@example.com SIP/2.0
To: <sip:friends@example.com >;tag=30
From: <sip:alice@example.com>;tag=12
Expires: 3600
Event: presence
Content-Length: 0
```

Obrázok 11: Hlavička metódy SIP SUBSCRIBE[15]

Ak je žiadosť určená pre prezenčný zoznam žiadosť bude smerovaná na RLS, ktorý udelí oprávnenie žiadosti užívateľa a odošle žiadosti jednotlivým užívateľom nachádzajúcim sa na prezenčnom zozname.

Akonáhle RLS (Resource List Server) autorizuje žiadosť užívateľa odošle ako odpoveď správu typu 200 OK a následne žiadosť NOTIFY s prázdny XML blokom (Obr.č.12) [15].



Obrázok 12: Proces SUBSCRIBE[15]

```

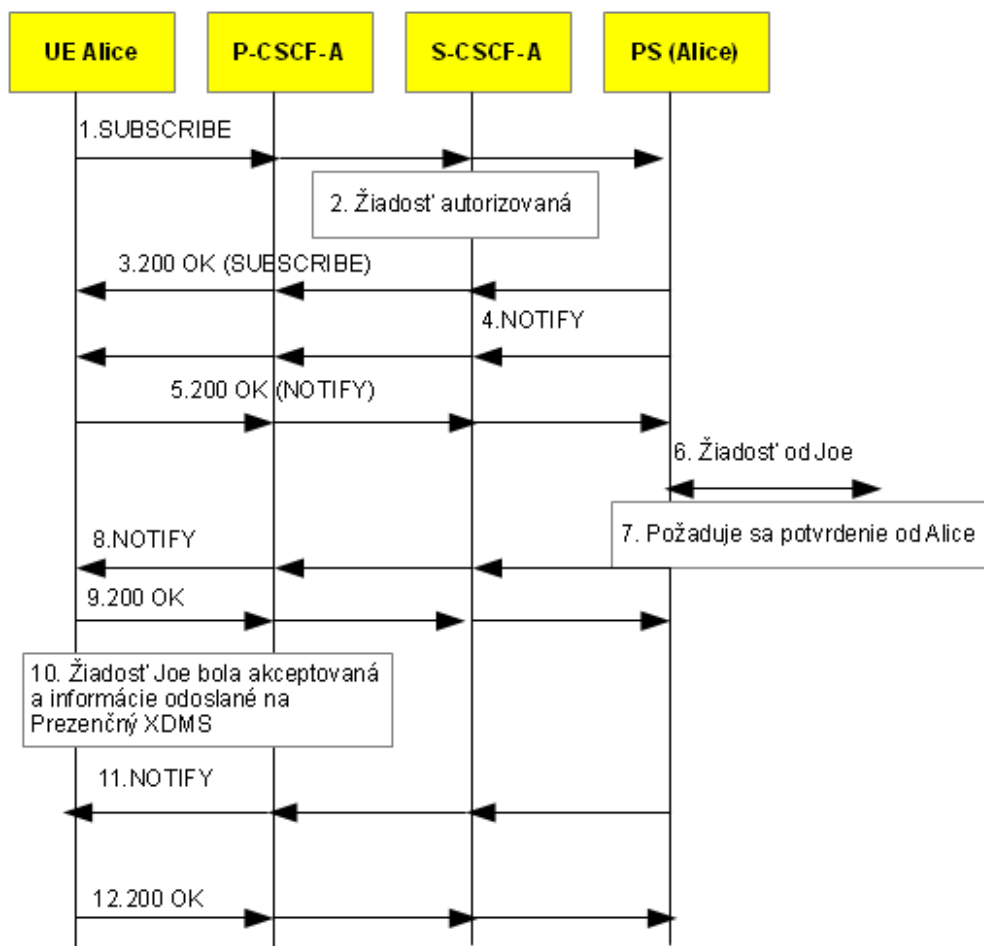
NOTIFY sip:alice@example.com SIP/2.0
To:<sip:alice@example.com>;tag=12
From: <sip:friends@example.com>;tag=30
Event: presence
Subscription-State: active;expires=3595
Content-Type: application/pidf+xml
Content-Length: ...
  
```

Obrázok 13: Hlavička metódy NOTIFY[15]

Po tom, čo RLS získa požadované prezenčné dáta z prezenčného serveru odošle NOTIFY, ktorá obsahuje požadované dáta v XML bloku (krok 14, Obr.č 12) [15].

4.5 Poskytnutie informácií o watcheroch

Na obrázku (Obr.č.14) je zobrazená situácia, kedy užívateľ (Alice) chce vedieť kto chce získať jej prezenčné informácie a následne rozhodne, či umožní prístup alebo nie.



Obrázok 14: Proces Watcher Information[15]

```

SUBSCRIBE sip:alice@example.com SIP/2.0
From: sip:alice@example.com;tag=123s8a
To: sip:alice@example.com
Event: presence.wininfo
    
```

Obrázok 15: Metóda SUBSCRIBE - presence.wininfo[15]

V kroku jedna (Obr.č.14) Alice odošle žiadosť SUBSCRIBE (Obr.č.15), žiadosť je smerovaná na S-CSCF server, ktorý spustí initial filter criteria, a zistí, že žiadosť sa týka watcher information, následne odošle na prezenčný server, ktorý prijme žiadosť. Týmto krokom užívateľovi Alice bude prezenčný server zasielať informácie o watcheroch. V kroku šesť sa užívateľ Joe (watcher) žiada o prezenčné informácie o Alice, prezenčný server mu oznámi, že je potrebné potvrdenie od Alice. A pretože Alice v kroku jedna zaslala žiadosť presence winfo,

server jej v kroku osem odošle NOTIFY (Obr.č.16) [15].

```
NOTIFY sip:alice@example.com SIP/2.0
From: sip:alice@example.com;tag=xyz887
To: sip:alice@example.com;tag=123s8a
Event: presence.winfo
Content-Type: application/watcherinfo+xml
Content-Length: ...
```

Obrázok 16: Metóda NOTIFY - presence.winfo[15]

Po obdržaní tejto správy terminál užívateľa Alice odošle na XDMS server pravidlá pre prístup k informáciám, následne server odošle informácie užívateľovi Joe a odošle NOTIFY užívateľovi Alice v kroku 11 [15].

5 IMS/TISPAN NGN výkonnostný test

IMS/NGN výkonnostné testy poskytujú informácie potrebné k návrhu, testovaniu a optimalizácii nových produktov, ktoré môžu zlepšiť výkonnosť IMS siete a kvalitu poskytovaných služieb zákazníkom [7].

Výkonnostnými testami sa napríklad simuluje populácia užívateľov využívajúca služby mobilných a telekomunikačných sietí, v našom prípade to bude IMS sieť.

Termíny výkonnostného testu:

Scenár a pokus o vykonanie scenára

Scenárom označujeme operáciu v rámci IMS, napríklad pokus o vytvorenie hovoru, registrácia, textové správy, interakcie medzi aplikáciami, prezenčné informácie a pod. Pokusom o scenár rozumieme moment, kedy je scenár spustený v IMS sieti. Scenár môže byť úspešný, neúspešný alebo funkcionálne úspešný, ale bude trvať dlhší čas ako je stanovené – v tom prípade sa vyhodnotí ako neúspešný ak je neúspešný označuje sa ako IHS(A) (Inadequately Handled Scenario Attempt). Scenáre môžu byť hovorovo závislé (konverzačné služby) a hovorovo nezávislé (registrácia, roaming). Avšak toto rozdelenie má význam len pre prvky siete, ktoré dokážu rozlíšiť typ scenára (napr. P- CSCF) [7].

DO (Design Objective)

Tento pojem označuje prijateľné percento IHSA pre daný scenár. Ak frekvencia IHSA presiahne Design Objective, potom DOC (Design Objective Capacity) bude prekročená [7].

Traffic-time profile

Je to pojem popisujúci priemernú rýchlosť pokusov o vykonanie scenára ako funkcia uplynutého času stanoveného pre výkonnostný test [7].

Traffic set

Je to kolekcia scenárov ktoré budú vykonávané, tak ako v reálnom prostredí [7].

Background load

Zaťaž aplikovaná na SUT počas výkonnostného testu za účelom spotreby výpočtových prostriedkov SUT (CPU, RAM).

Test parameters

Parametre testu sa využívajú pre kontrolu testovacieho skriptu. Dátové prvky, ktoré treba nakonfigurovať v TS sú v tabuľke (tabuľka č.1) [7].

Tabuľka 1. Parametre testu

Parameter	Typ	Popis
PX_TotalProvisionedSubscribers	Integer [-]	Počet simulovaných účastníkov v sieti
PX_PercentRegisteredSubscribers	Integer [%]	Priemerné percento účastníkov, ktorí sú registrovaný súčasne
PX_StepNumber	Integer [-]	Počet krokov v teste
PX_StepTime	Float [s]	Čas, počas ktorého je spustený test na danej úrovni SIP záťaže
PX_System Load	Integer [SAPS]	Rýchlosť pokusov o vykonanie scenára
PX_StirTime	float [s]	Čas, počas ktorého je SUT vystavený SIP záťaži, avšak niesú zbierané dáta. (v našom prípade t1,t3)(Obr.č.18)
PX_SAPSIncreaseAmount	Integer [-]	Krok zvyšujúci vykonávaný počet scenárov
PX_PercentRoamingSubscribers	Integer [%]	Počet percent užívateľov využívajúci roaming
PX_StepTransientTime	Float [-]	Interval od začiatku kroku počas, ktorého nie sú počítané pokusy o scenár

5.1 Test – Bed

Pojmom test – bed označujeme prostredie nakonfigurované pre testovanie, môže sa skladať z konkrétného hardvéru, softvéru, operačného systému, sieťovej topológie, konkrétnej konfigurácie, zariadený podľa potreby a iných aplikácií nevyhnutných pre testovanie daného systému.

5.2 SUT (System Under Test)

SUT označujeme systém, ktorého funkcionality budú testované. Pretože IMS sieť sa skladá z rôznych blokov (subsystémov) ako blok riadenia relácií (CSCF), blok medzi sieťovej komunikácie (BGCF), databázy (HSS, SLF), blok poskytovania služieb užívateľom (AS). Preto sa aj IMS/NGN výkonnostné testy uskutočňujú pre jednotlivé subsystémy. IMS/NGN prvky, ktoré nie sú zahrnuté v testovanom subsystéme sú označované ako prostredie vykonávaného testu, ktoré musí byť prítomné pre zaistenie funkcionality testovaného subsystému, ale toto prostredie nie je predmetom výkonnostného testu [8].

5.2.1 Základňa užívateľov

Pre SUT je nutné definovať základňu užívateľov. Mala by obsahovať:

- Doménu – všetky verejné a súkromné identity budú používať rovnakú doménu
- Počet účastníkov
- Účastník – každému účastníkovi je pridelená jedna súkromná identita a jedna verejná identita
 - Súkromná identita:

Username – validne username začínajúc sa PrivateId. Minimálna, maximálna dĺžka identity.

Doménu

Použiteľné znaky

Algoritmus – autentifikačný algoritmus, ktorý užívatelia používajú

K – tajný kľúč pre užívateľa

- Verejná identita :

Validnu SIP URI, rovnako ako pri súkromnej identite.

Doména

- ID Mapovanie

Verejné ID

Súkromné ID [8]

5.2.2 SUT parametre a konfigurácia

Tento element test – bedu popisuje presný zoznam hardvéru, softvéru a ich konfigurácie, z ktorého je SUT zostavený, taktiež obsahuje parametre spojenia s test system (šírka pásma, oneskorenie, zabezpečenie a pod.). Je to nutné z dôvodu, aby mohol byť testovaný systém opakovateľný [8].

5.3 TS (Test System)

Je systém (hardware, software), ktorý generuje záťaž a požiadavky (traffic) na SUT.

5.3.1 TS parametre a konfigurácia

Presný zoznam hardvéru, softvéru a ich konfigurácie, z ktorého je TS zostavený. Taktiež je nevyhnutné uviesť presný popis skúšobného testu (v našom prípade testovanie služby sledovania dostupnosti klientov) pre potreby opakovania test systému na rovnaký SUT. Ak bol počas skúšobného testu použitý systém pre generovanie backgroun load pre zaistenie

spotreby prostriedkov SUT treba uviesť presný opis tohto systému [8].

5.4 Zaznamenávané parametre výkonnostného testu

Parametre testu môžu byť vyhodnocované počas priebehu testu alebo môžu byť vyhodnotené po skončení testu zo záznamov udalostí (event logs) vytvorených počas skúšky. Parametre by mali byť zaznamenávané formou: skratka, celý názov, popis, jednotky, prostriedky použité na záznam, účel. Zaznamenávané parametre môžu byť: IHS, MEM, CPU, SIMS a SAPS [8][9].

5.4.1 IMS/KPI Úspešnosť počiatkovej registrácie S – CSCF

Toto KPI (Key Performance Indicator) vyjadruje počet úspešne vykonaných registrácií k počtu celkovo vykonaných registrácií, vykonaných serverom S – CSCF. Týmto parametrom sa vyhodnocuje výkonnosť prístupu k IMS sieti [13].

$$IRSR = \frac{\sum UR.SuccInitReg}{\sum UR.AttInitReg} * 100 [13] .$$

5.4.2 IHS (Inadequately Handled Scenario) parameter

IHS parameter sa vyhodnocuje ako podiel sumy neúspešných scenárov (pod pojmom scenár rozumieme napríklad pokus o vytvorenie hovoru, registráciu a podobne) a sumy úspešných plus sumy neúspešných scenárov: $\% IHS = \frac{\sum failed}{(\sum succeeded + \sum failed)}$ [7]. Neúspešný scenárom rozumieme napríklad prekročenie stanoveného oneskorenia a prahových hodnôt, zlyhanie vytvorenia hovoru, registrácie a pod.

5.5 Vlastná architektúra IMS siete a test – bedu

V našom prípade testovaný systém (SUT) bude predstavovať implementácia IMS siete skladajúca sa z prvkov S – CSCF, P – CSCF, I – CSCF, HSS, prezenčného servera, XDMS servera a DNS servera (Obr.č.17). Výkonnostný test bude vykonaný pre subsystém poskytovania služieb zákazníkom, teda pre aplikačné servery (Prezenčný server a XDMS server) a pre P/S – CSCF subsystém. Doména IMS siete bude **kamailio.ims.network**. Test System (TS) bude realizovaný pomocou softvéru LxLoad od Ixia. Pre spotrebu výpočtových prostriedkov prvkov siete bude využitá umelá záťaž CPU. Testom bude meraná doba spracovania žiadostí prvkami P – CSCF, S – CSCF a aplikačnými servermi.

5.5.1 Ixia LxLoad

LxLoad je škálovateľné riešenie pre testovanie konvergovaných služieb, aplikácií donáškových platforiem a bezpečnostných zariadení a systémov. LxLoad emuluje, hlas, video účastníkov a

stým súvisiace protokoly pre zabezpečenie QoE (quality of experience). Rovnako dokáže simulovať malware a DDoS (distributed denial of service) útoky pre testovanie bezpečnosti [11].

5.5.2 Kamailio open source SIP server

Pomocou Open Source SIP Server Kamailio budú realizované prvky: S – CSCF, P – CSCF, I – CSCF. Návod na inštaláciu je na stránkach Žilinskej univerzity [19].

Kamailio™ (bývalý OpenSER) je Open Source SIP Server vydaný pod GPL (General Public Licence), ktorý je schopný zvládnuť tisícky hovorov za sekundu. Medzi jeho funkcie patrí: asynchrónne TCP, UDP a SCTP zabezpečená komunikácia pomocou TLS pre VoIP (hlas, video), IPv4 a IPv6, SIMPLE instant messaging a prezencia so vstavaným XCAP serverom a MSRP, ENUM, DID a Least Cost Routing, load balancing, smerovanie fail-over, vyúčtovanie, autentizáciu a autorizáciu, podpora MySQL, Postgres, Oracle, Radius, LDAP, Redis, Cassandra, XMLRPC riadiace rozhranie SNMP monitorovanie. Kamailio môže byť použitý na budovanie veľkých VoIP servisných platforiem alebo rozšíriť SIP-to-PSTN brány, PBX systémy alebo mediálne servery ako Asterisk™, FreeSWITCH™ alebo SEMS. Kamailio a SIP Express Router (SER) sa spojil pre integráciu oboch aplikácií a novým vývojom.

Kamailio môže byť použitý v systémoch s obmedzenými zdrojmi, rovnako ako v chrbticových serveroch. Je napísaný v jazyku C pre Unix/Linux-ako systémy s optimalizáciou architektúry ponúkajú veľký výkon. Kamailio projekt si kladie za cieľ byť kolaboratívne prostredie svojich užívateľov na rozvoj bezpečného a rozšíriteľného SIP servera, poskytovať modernú jednotnú komunikáciu a VoIP služby [12].

5.5.3 Umelá záťaž CPU

Spotreba výpočtových prostriedkov SUT bude uskutočnená open source programom lookbusy. Tento program bude nainštalovaný na prvkoch P – CSCF, S – CSCF a aplikačných serveroch. [18]. Táto aplikácia je zvolená z dôvodu, že umožňuje umelé zaťaženie nielen CPU, ale aj operačnej pamäte a hard disku. V prípade potreby experimentu môžeme dodatočne využiť aj tieto funkcie.

5.5.4 FHoSS Open IMS Core

Na základe projektu Open IMS Core bude realizované: HSS (FhoSS). HSS z projektu Open IMS Core je použité preto, že projekt kamailio neobsahuje implementáciu HSS. Návod na inštaláciu nájdeme znova na stránkach Žilinskej univerzity [19].

Open IMS Core je Open Source implementácia IMS Call Session Control Functions (CSCF) a Home Subscriber Sercer (HSS), ktoré spolu tvoria základné prvky IMS/NGN architektúry, ako je to v súčasnosti špecifikované v 3GPP, 3GPP2, ETSI TISPAN a v PacketCable [14].

5.5.5 OpenXCAP

Prezenčný a XDMS server bude realizovaný pomocou OpenXCAP serveru [3].

OpenXCAP je open source XCAP server. Server XCAP používajú klienti SIP a slúži pre manažovanie buddy listov a politiky pre žiadosti o prezenčné služby alebo iný tip udalosti používajúcej SIP protokol. Je licencovaný podľa GPL verzie 2 [3].

5.5.6 Popis navrhnutej architektúry IMS siete a test-bedu

Navrhnutá architektúra pre test-bed je na obrázku (Obr.č.17). Samotná IMS sieť bude zostavená len z prvkov P – CSCF, I – CSCF, S – CSCF, HSS, DNS, prezenčného a XDMSservera. Tieto prvky dostatočne postačia na realizáciu IMS siete a vykonanie test-bedu prezenčnej služby dostupnosti jednotlivých klientov poskytovanej aplikačnými servermi (prezenčný a XDMS server).

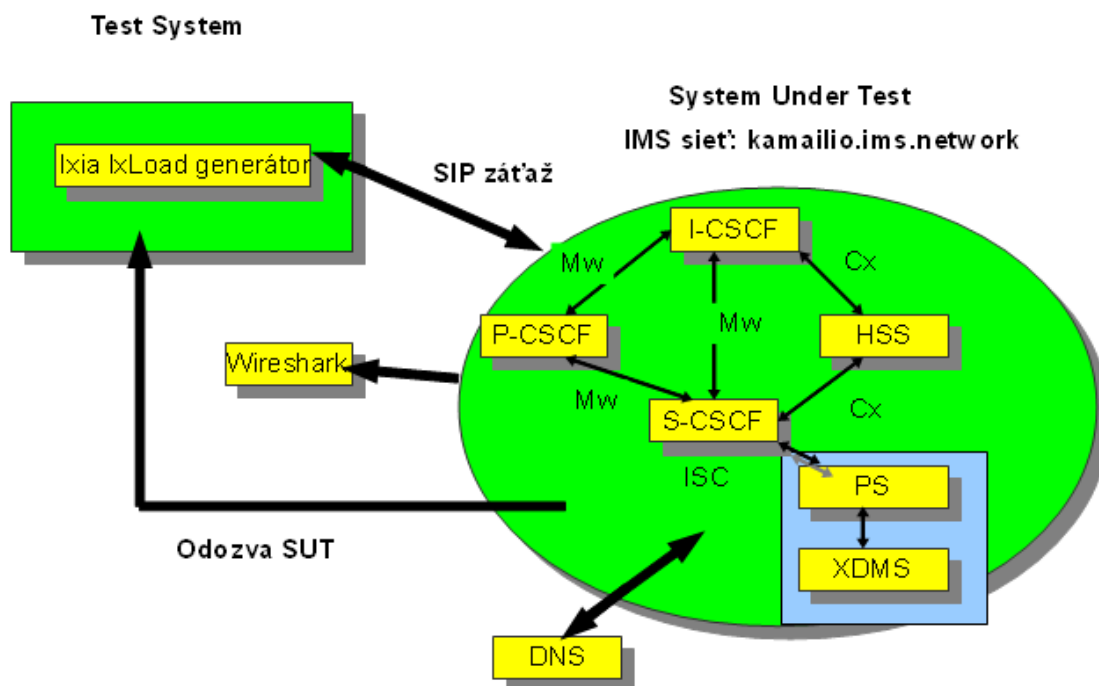
V implementácii IMS siete nie je použitá SLF databáza, ktorá obsahuje odkazy na HSS databázy a využíva sa len prípadne, ak sieť obsahuje viac ako jednu databázu HSS. V našom prípade postačí jedna databáza HSS, pretože počet vytvorených užívateľov bude zanedbateľný s kapacitou HSS.

Sieť ďalej neobsahuje aplikačné servery ako OSA -SCS a IM-SSF. OSA-SCS server slúži pre komunikáciu s OSA serverom a umožňuje sprístupnenie služieb v IMS sieti navrhnutých pre OSA servery. Takéto služby nebudú v teste využívať. IM-SSF server sprístupňuje CAMEL služby využívané v GSM sieťach užívateľom IMS siete, takýto typ služby taktiež nebudú využívať.

Nie sú použité ani prvky BGCF , IMS-ALG, SGW, MGCF, TrGW a MGW. Tieto prvky zabezpečujú medzisieťovú komunikáciu, medzi IMS sieťou a PSTN, PLMN, medziprotokolovú komunikáciu IPv4 a Ipv6 a preklad medzi signalizáciou založenej na IP protokole a SCTP/IP, SS7 protokoloch. Naša sieť bude používať protokol IPv4.

Prvok MRF taktiež nebude použitý, zabezpečuje transkódovanie medzi odlišnými kodekmi a zmiešava multimediálne toky dát od rôznych užívateľov za účelom vytvorenia konferenčného hovoru.

Koncový užívateľia budú simulovaní pomocou Ixia IxLoad, ktorí budú zasielať rôzne SIP žiadosti (scenáre) na SUT.



Obrázok 17: Architektúra Test-bedu

Tabuľka 2. Informácie o navrhutej architektúre IMS siete

Doména	Uzol siete	Operačný systém	IP adresa:Port
kamailio.ims .network	P-CSCF	Ubuntu 12.10	192.168.1.67:4060
	I-CSCF	Ubuntu 12.10	192.168.1.68:5060
	S-CSCF	Ubuntu 12.10	192.168.1.66:6060
	HSS	Ubuntu 12.10	192.168.1.65:8080
	DNS	Ubuntu 12.10	192.168.1.68:53
	TS IxLoad	Windows xp	192.168.1.22:5060
	PS a XDMS	Ubuntu 12.10	192.168.1.40:5090

Tabuľka 3. Zaznamenávané parametre a analýza dát výkonnostného testu

Skratka	Celý názov	Popis	Jednoty	Analýza dát	Účel
SAPS*	Scenario Attempts Per Second	Preimerné množstvo pokusov o scenár za sekundu	/	TS:reporty z IxLoad ixia SUT:Wireshark	Poskytuje spôsob ako definovať záťaž na SUT
TRT	Transaction Response Time	Doba spracovania žiadosti prvkami siete	ms	TS:reporty z IxLoad ixia SUT:Wireshark	Meranie doby spracovania transakcií
SIMS	Simultaneous Scenario	Počet súčasne aktívnych scenárov	/	TS:reporty z IxLoad ixia SUT:Wireshark	Vplyv súčasne aktívnych scenárov
%IHS	Percent Inadequately Handled Scenarios	Počet neúspešných scenárov k počtu úspešných scenárov	%		Poskytuje informácie o DOC

*SAPS je vstupný parameter

Vyhodnocovaný scenár:

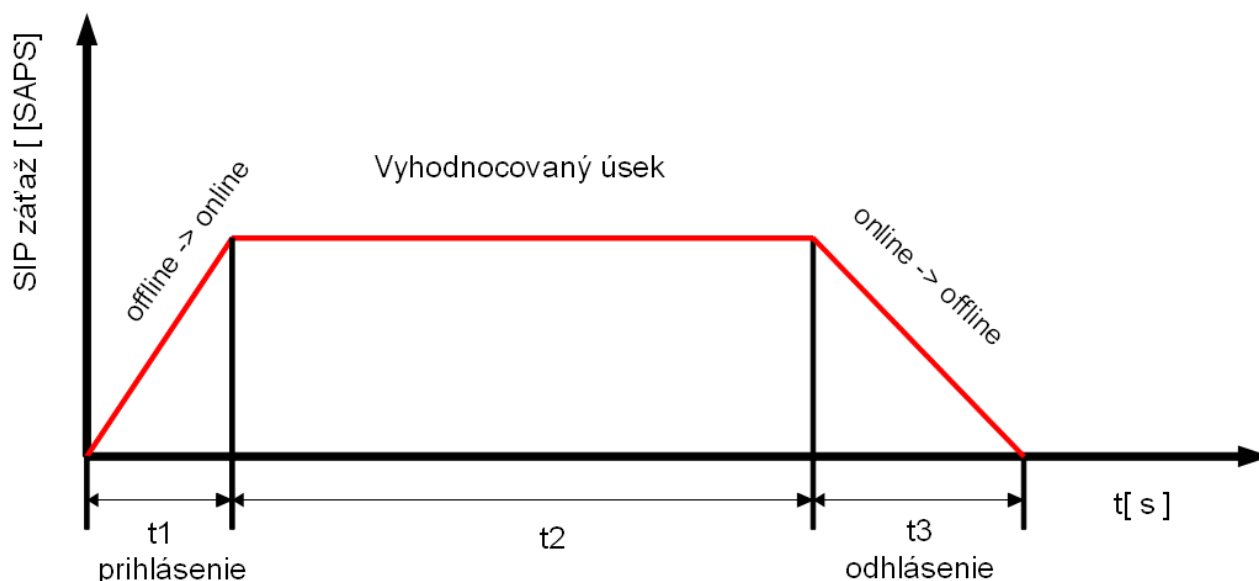
- Prezenčná služba, poskytnutie informácií o termináli a klientoch.
 - osobné informácie klientov
 - možnosti terminálu (MMS, Video, podpora POC)
 - dostupnosť terminálu

Scenár bude simulovaný v TS pomocou IxLoad ixia.

Tabuľka 4. Navrhnutá základňa užívateľov

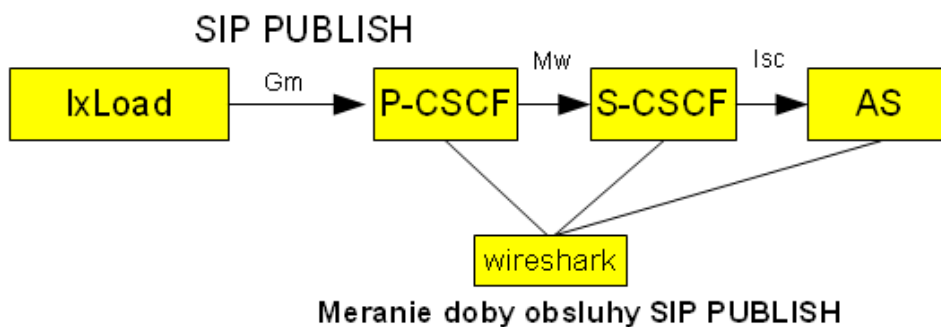
Názov	Hodnota
Dĺžka názvu domény	20
Doména	kamailio.ims.network
Počet užívateľov	10000
Min. dĺžka súkromného ID	4
Max. dĺžka súkromného ID	20
Prijateľné znaky súkromného ID	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
Algoritmus súkromného ID	Digest-AKAv1-MD5
K hodnota súkromného ID	0x6162636465666768696a6b6c6d6e6f70
Min. dĺžka verejného ID	4
Max. dĺžka verejného ID	20
Prijateľné znaky verejného ID	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789

Na obrázku (Obr.č.18) je zobrazená doba vyhodnocovania vykonaného testu. V čase t_1 nastáva prihlásenie užívateľov do siete a zase naopak v dobe t_3 nastáva odhlásenie užívateľov zo siete. Pri prihlásení a odhlásení nastáva zmena statusu užívateľov, sú vyslané správy SIP PUBLISH a tým pádom oznámenie ostatným užívateľom o zmene statusu. Tieto operácie tiež patria medzi prezenčné služby, avšak nebudú brané do úvahy pri vyhodnotení testu a to z dôvodu, že táto operácia je nevyhnutná na prístup a komunikáciu v IMS sieti a musí ju vykonať každý užívateľ. Vyhodnocovaný úsek bude v čase t_2 . Doba t_2 bude 30 minút.



Obrázok 18: Doba a úsek vyhodnocovania testu

Obrázok č.19 zobrazuje tok správy PUBLISH, pri zmene statusu užívateľa alebo terminálu (prezenčná služba). Programom wireshark sa bude merať doba obsluhy správy jednotlivými prvkami. Pri prezenčných službách sú generované aj SIP správy SUBSCRIBE a NOTIFY (viď kap. 4.3, 4.4 a 4.5), ktorých tok sieťou je zhodný ako so správou SIP PUBLISH zobrazený na obrázku (Obr.č.19).



Obrázok 19: Tok správy PUBLISH sieťou

5.5.7 Pribeh meraní

1. Zistí sa maximálna SIP záťaž, ktorou je možné vyťažiť celkový systém na 30 minút tak, aby nedošlo k “spadnutiu” procesov na serveroch zabezpečujúcich funkciu prvkov IMS siete.
2. Po tom, ako sa zistí maximálna záťaž (očakávaná hodnota bude niekde medzi 500-1000 SAPS), sa určia hodnoty SAPS, pre ktoré budú spustené testy (napr. 100, 200, 300 maximálna hodnota). Maximálna hodnota, ktorou je možné zaťažiť systém bude overená 10 meraniami (10 meraní bude vykonaných z dôvodu upresnenia hodnoty, pretože sa môže stať že systém raz spadne pri inej hodnote a inokedy zasa pri inej, z meraní bude spravený priemer, ktorý sa zaokrúhly na stovky). Zistená maximálna hodnota SAPS nebude počast testov prekročená.
3. Pre každú zvolenú hodnotu SAPS (100, 200, 300, ...max.) sa zistí vyťaženie CPU každého prvku siete bez umelého vyťaženia programom lookbusy. Meranie sa bude opakovať pre každú hodnotu SAPS 10-krát. Z nameraných hodnôt pre každú hodnotu SAPS sa spraví priemer. Táto hodnota bude braná ako minimálna hodnota zaťaženia prvku (označovaná ako MIN_CPU).
4. Bude vykonané meranie doby obsluhy SIP správ PUBLISH, SUBSCRIBE, NOTIFY (správy súvisiace z prezenčnými službami) a to spôsobom že k hodnote MIN_CPU každého prvku sa bude pripočítavať umelá záťaž, realizovaná programom lookbusy. Pri zvolenej SIP záťaži z bodu 2. Meranie sa vykoná 10-krát.

Nastavovanie umelej záťaže CPU:

- $\text{MIN_CPU} + 10\% * \text{MIN_CPU}$ (výsledná hodnota bude zaokrúhlená na 5%, tj. v prípade, že sa bude jednať o 21%, bude to 20%, v prípade, že sa bude jednať o 24%, bude nastavená hodnota 25%).
- $\text{MIN_CPU} + 20\%$,dovtedy kým $\text{MIN_CPU} + n < 100\%$, n = krok zvyšovania záťaže (10%, 20%, 30%,90-95%).

(V prípade časových možností, bude z dôvodu väčšej štatistickej presnosti uskutočnených viac ako 10 meraní).

Namerané výsledky budú spracované graficky nasledovným spôsobom:

1. Grafický priebeh závislosti vytťaženia CPU (os y) na SAPS (os x) pre všetky sledované prvky IMS siete.
2. Grafický priebeh závislosti doby obsluhy (os y) správ SIP PUBLISH, SIP SUBSCRIBE, SIP NOTIFY pre hodnoty MIN_CPU a zistenej maximálnej SIP záťaži pre každý prvok IMS siete (os x).
3. Grafický priebeh závislosti doby obsluhy (os y) správ SIP PUBLISH, SIP SUBSCRIBE, SIP NOTIFY pre rôzne hodnoty záťaže CPU (os x) s konštantnou SIP záťažou a pre rôzne hodnoty SIP záťaže (os x) s konštantným zaťažením CPU pre každý prvok IMS siete. Táto závislosť ukáže, čo má väčší vplyv na dobu spracovania správy, CPU zaťaženie alebo SIP zaťaženie.

6 Inštalácia, chyby pri inštalácií a oživovaní IMS siete

6.1 Kamailio 3.3.2 Open source SIP server

6.1.1 Inštalácia

SIP server Kamailio je vytvorený pre operačné systémy na báze Linuxu. Ja som zvolil operačný systém Ubuntu 12.04.

Pred samotným stiahnutím a inštaláciou je nutné si stiahnuť verejný kľúč a pridať si ho medzi ostatné kľúče:

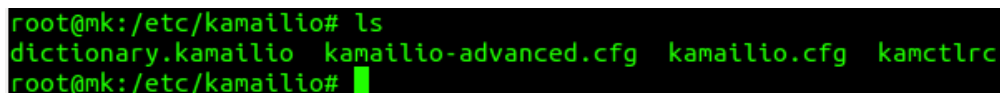
```
wget http://repository.ng-voice.com/PublicKey  
apt-key add PublicKey
```

Následne môžeme pridať repozitár, z ktorého sa automaticky stiahne a nainštaluje Kamailio a ims moduly :

```
deb http://repository.ng-voice.com squeeze ims  
apt-get install kamailio  
apt-get install kamailio-ims-modules
```

Týmto sa nainštaloval základný SIP server a ims moduly, ktorého funkcionality (I – CSCF, P – CSCF, S – CSCF alebo XCAP & Prezenčný server) môžeme meniť v závislosti od spúšťaného konfiguračného súboru a jeho úpravy.

Defaultné konfiguračné súbory sa nainštalujú do zložky `/etc/kamailio` (Obr.č20).



```
root@mk:/etc/kamailio# ls  
dictionary.kamailio kamailio-advanced.cfg kamailio.cfg kamctlrc  
root@mk:/etc/kamailio#
```

Obrázok 20: Cesta k defaultným konfiguračným súborom

Konfiguračné súbory pre jednotlivé prvky I – CSCF, P – CSCF, S – CSCF sú uložené v zložke : `/usr/share/doc/kamailio/examples/` (Obr.č.21) . Tam rozbalíme súbor `kamailio.cfg.gz` a spolu so súbormi `xcscf.cfg` a `xcscf.xml` ich kopírujeme do zložky `/etc/kamailio`.

```

root@mk:/usr/share/doc/kamailio/examples# ls
acc.cfg          exec_s5b.cfg    onr.cfg          snmp.cfg
ccdiversion.cfg  exec_s5.cfg     pcscf            uas.cfg
ctd.sh.gz        flag_reply.cfg  pi_framework.xml.gz  vm_proxy.cfg
exec.cfg          geo_split.sh    pstn.cfg.gz      voicemail.cfg
exec_dist.cfg     icscf           redirect.cfg      web_im
exec_s2.cfg       kamailio        replicate.cfg     websocket.cfg.gz
exec_s3.cfg       logging.cfg     scscf            welcome.cfg
exec_s4.cfg       msilo.cfg       serial_183.cfg    xhttp.cfg
root@mk:/usr/share/doc/kamailio/examples# cd pcscf/
root@mk:/usr/share/doc/kamailio/examples/pcscf# ls
kamailio.cfg  kamailio.cfg.gz  pcscf.cfg  pcscf.xml  tls.cfg
root@mk:/usr/share/doc/kamailio/examples/pcscf# █

```

Obrázok 21: Konfiguračné súbory serverov CSCF

Súbor `xcscf.cfg` je importovaný do súboru `kamailio.cfg`, ktorý je spúšťaný. `Xcscf.cfg` slúži na nastavenie portu, IP adresy a domény serveru. Súbor `xcscf.sml` slúži na nastavenie komunikácie z HSS databázou cez protokol DIAMETER.

Príkazy pre prácu s kamailiom :

`man kamailio` (zobrazí manuál)

`kamailio -c` (spustí konfig z názvom `kamailio.cfg` a kontroluje či obsahuje chyby)

`kamailio -d` (debuging)

`kamailio -f súbor` (spustí kamailio zo zadaným konfigom)

6.1.2 Chyby pri spúšťaní P-CSCF

Pri pokuse o spustenie servera P – CSCF došlo k chybám.

```

root@mk:/etc/kamailio# kamailio
loading modules under /usr/lib64/kamailio/modules_k/:/usr/lib64/kamailio/modules
/:/usr/lib/kamailio/modules_k/:/usr/lib/kamailio/modules/
ERROR: bad config file (33 errors)
root@mk:/etc/kamailio#

```

Obrázok 22: Chyby pri spustení P - CSCF

Pri nastavení debugu a zadaní príkazu `kamailio -d` nám vypíše podrobnejšie chyby, ktoré môžu byť opravené.

Na opravu chýb je nutné v konfiguračnom súbore zakomentovať riadky:

```

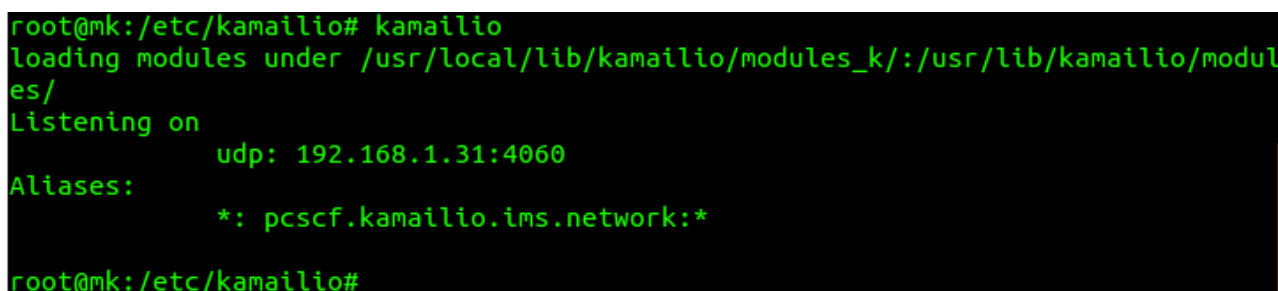
#loadmodule "pua"
#loadmodule "db_sqlite"
# ----- pua params -----
# Database is disabled (for now)
#modparam("pua", "db_mode", 0)

```

```
#modparam("pua","db_url","sqlite:///etc/kamailio/kamailiodb")
")
```

Ďalej je nutné nainštalovať kamailio-xml-modules a kamailio-xmllrpc-modules. Tie ale vyžadujú balíčky libxmllrpc-c3 a libxmllrpc-core-c3. Najskôr sa musí nainštalovať balík libxmllrpc-core-c3, aby sa predišlo ďalším chybám.

Po týchto úpravách ide server spustiť bez problémov (Obr.č.23).

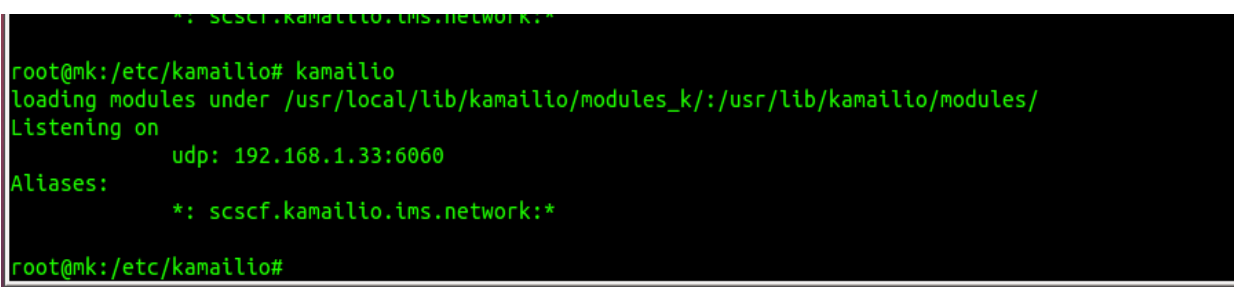


```
root@mk:/etc/kamailio# kamailio
loading modules under /usr/local/lib/kamailio/modules_k:/usr/lib/kamailio/modules/
Listening on
      udp: 192.168.1.31:4060
Aliases:
      *: pcscf.kamailio.ims.network:*
root@mk:/etc/kamailio#
```

Obrázok 23: Spustenie P - CSCF

6.1.3 Spustenie S – CSCF

Tento server išiel spustiť bez problémov.



```
root@mk:/etc/kamailio# kamailio
loading modules under /usr/local/lib/kamailio/modules_k:/usr/lib/kamailio/modules/
Listening on
      udp: 192.168.1.33:6060
Aliases:
      *: scscf.kamailio.ims.network:*
root@mk:/etc/kamailio#
```

Obrázok 24: Spustenie S - CSCF

6.1.4 Spustenie I – CSCF

Server I – CSCF vyžaduje doinštalovanie mysql serveru a install kamailio-mysql-modules.

```
apt-get install kamailio-mysql-modules
apt-get install mysql-server
apt-get install libmysqlclient15off
```

Ďalej je treba nutné vytvoriť databázu a užívateľa, ktorému pridáme práva:

```
mysql -uroot -p
mysql> create database icscf;
```

```
mysql> CREATE USER 'icscf'@'localhost' IDENTIFIED BY 'secret';
```

```
mysql> GRANT ALL PRIVILEGES ON icscf.* TO 'icscf'@'localhost';
```

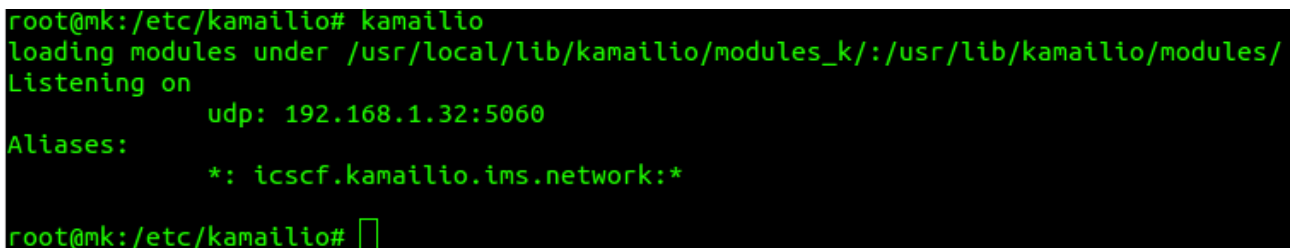
Ďalej musí byť upravený súbor `icscf.sql`, ktorý sa nachádza v zložke `/usr/share/doc/kamailio/examples/icscf`, v ňom sa prepíše názov domény a port.

Následne ho príkazom `mysql -uroot -p icscf < icscf.sql` importujeme do databázy.

Po týchto úpravách pri pokuse o spustenie server vypisoval chybu, že nemôže nájsť cestu k databáze. Chyba sa odstráni prepísaním riadka v súbore `icscf.cfg`.

```
#!/define DBURL "mysql://icscf:secret@localhost/icscf"
```

Po tejto úprave server ide spustiť (Obr.č25).



```
root@mk:/etc/kamailio# kamailio
loading modules under /usr/local/lib/kamailio/modules_k:/usr/lib/kamailio/modules/
Listening on
udp: 192.168.1.32:5060
Aliases:
*: icscf.kamailio.ims.network:*
root@mk:/etc/kamailio#
```

Obrázok 25: Spustenie I - CSCF

6.1.5 Nefunkčnosť Prezenčného a XCAP serveru

Na tento server sa musia doinštalovať potrebné moduly:

```
apt-get install mysql-server
```

```
apt-get install kamailio-mysql-modules
```

```
apt-get install kamailio-presence-modules
```

Webové rozhranie Siremis k XCAP serveru vyžaduje nainštalovanie apache serveru. Cez toto rozhranie sa dá manažovať Prezenčný a XCAP server. Na obrázku je vidieť vytvorený zoznam watcherov (Obr.č.26).

```
apt-get install apache2 apache2-doc
```

```
a2enmod rewrite
```

```
apt-get install php5 php5-mysql php5-gd
```

```
wget
```

<http://siremis.asipto.com/pub/downloads/siremis/siremis-2.0.0.tgz>

Id	Presentity Uri	Watcher Username	Watcher Domain	Event	Inserted Time
1	sip:alice@kamailio.ims.network	martix	kamailio.ims.network	presence	134550
2	sip:martix@kamailio.ims.network	alice	kamailio.ims.network	presence	134740
3	sip:martin@kamailio.ims.network	alice	kamailio.ims.network	presence	4561

Obrázok 26: Rozhranie Siremis, zoznam watcherov

Po nainštalovaní všetkých potrebných modulov otvoríme a upravíme súbor `/etc/kamailio/kamctlrc`. Je to súbor, ktorý vytvára kamailio databázu. Po jeho úprave sa vytvorí príkazom `kamdbctl create kamailio` databáza. Správnosť overíme výpisom, ktorý by mal byť: `INFO: Core Kamailio tables succesfully created.`

Konfiguračný súbor tohto servera taktiež vyžadoval úpravy a však aj po úpravách sa server nedal spustiť. V konfiguračnom súbore som odkomentoval moduly, ktoré si mal server načítať a pridal časti kódu, ktoré zabezpečovali funkcionality prezenčného a XCAP servera. Aj po ich od-komentovaní a vložení časti kódu do konfiguračného súboru server vypisoval chybu, že mu chýba daný modul, ale keď som skontroloval cestu odkiaľ si načítava daný modul, tak cesta bola v poriadku a nachádzal sa tam aj daný modul. Dopĺňaný kód bol z oficiálnej stránky kamailia <http://www.kamailio.org/dokuwiki/doku.php/presence:configuration-file>. Nepomohla ani opätovná inštalácia.

```
loadmodule "mi_rpc.so"
#loadmodule "acc.so"
loadmodule "presence.so"

#ifdef WITH_AUTH
loadmodule "auth.so"
loadmodule "auth_db.so"
```

Obrázok 27: Modulv serveru v konfiguračnom súbore

```
counters.so      matrix.so      presence.so    siptrace.so     usrloc.so
ctl.so           maxfwd.so     presence_xml.so siputils.so      xcap_client.so
db2_ops.so       mediaproxy.so pua_bla.so     sl.so           xcap_server.so
db_cluster.so    mi_datagram.so pua_dialoginfo.so sms.so          xhttp_rpc.so
db_flatstore.so  mi_fifo.so    pua_mi.so      speeddial.so    xhttp.so
db_text.so       mi_rpc.so     pua_reginfo.so sqlops.so       xlog.so
debugger.so      mqueue.so     pua.so         sst.so          xprint.so
dialog.so        msilo.so      pua_usrloc.so  statistics.so
root@mk:/usr/lib/kamailio/modules#
```

Obrázok 28: Modulv serveru

```
root@mk:/etc/kamailio# nano kamailio.cfg
root@mk:/etc/kamailio# kamailio -d
loading modules under /usr/local/lib/kamailio/modules_k:/usr/lib/kamailio/modules/
Segmentation fault (core dumped)
root@mk:/etc/kamailio#
```

Obrázok 29: Chyba pri spustení serveru

Samotnú sieť IMS sa mi podarilo rozbehnúť ale bez prezenčného servera, a aj samotná IMS na báze Kamailia bola nestabilná a bez príčin vypadávali servery.

6.2 Open IMS Core

Po neúspechu s platformou Kamailio, ktoré bolo celkovo problémové od počiatočného získania verejného kľúča pre možnosť pridania repozitárov a automatickej inštalácie, až po spúšťanie jednotlivých prvkov CSCF a ich nestabilitu, som sa rozhodol, že na svoju prácu použijem starší a stabilnejší projekt Open IMS Core, avšak prezenčný server sa mi nepodarilo sprevádzkovať ani na tejto platforme.

6.2.1 Inštalácia

Túto platformu som inštaloval na rovnaký operačný systém ako kamailio teda Ubuntu 12.04. Zo stránky <http://www.openimscore.org/download> si stiahneme zdrojové kódy jednotlivých prvkov CSCF a inštalujeme podľa návodu na stránke http://www.openimscore.org/installation_guide. Kódy sťahujeme cez program SubVersion:

```
svn checkout svn://svn.berlios.de/openimscore/ser_ims/trunk
svn checkout svn://svn.berlios.de/openimscore/JavaDiameterPeer/trunk
svn checkout svn://svn.berlios.de/openimscore/CDiameterPeer/trunk
```

Prejdeme do priečinka, kam sme si stiahli zdrojové kódy a príkazom `make install-libs all` spustíme kompiláciu. Po úspešnej kompilácii nastavíme jednotlivé prvky CSCF a to pomocou súboru `.cfg`, `.sh`, `.xml`. Jednotlivé prvky sa spúšťajú pomocou súborov s príponou `.sh`

6.2.2 Chyba prezenčného servera openSIPS 1.5.0 without tls

Rovnako ako v predošlom prípade sa do konfiguračného súboru dopĺňal kód, ktorý zabezpečoval funkcionality prezenčného servera. Po vložení kódu však server nešiel spustiť (Obr.č.30). Vo výpise chyby je napísané, že súbor s príponou `.pid` neexistuje. Tento súbor si server vytvára pri správnom spustení. Jediné riešenie, ktoré som zistil je, že nie je vytvorený priečinok v zložke `/var/run/` s názvom `opensips`, ale ten vytvorený bol.

```
fifo ..... send raw FIFO command
root@mk:/usr/local/etc/opensips# opensipsctl start
INFO: Starting OpenSIPS :
ERROR: PID file /var/run/opensips/opensips.pid does not exist -- OpenSIPS start
failed
root@mk:/usr/local/etc/opensips#
```

Obrázok 30: Chyba prezenčného servera Opensips

7 Boghe IMS klient

Boghe IMS je voľne šíriteľný IMS klient vydaný pod GNU General Public License, ktorý poskytuje množstvo funkcií v rámci IMS siete. Pre testy som zvolil práve tohto klienta.



Obrázok 31: Boghe IMS/RCS client

8 Metodika testovania

Pre nestabilnosť riešenia a nefunkčnosti prezenčného servera bola po konzultácii z vedúcim práce dodatočne vybraná služba VoIP.

Testy boli vykonávané na IMS sieti pozostávajúcej zo CSCF serverov, HSS databázy, DNS serveru a dvoch klientských staniciach s IMS klientom Boghe IMS/RCS. Všetky testy boli vykonávané na základe RFC 6076, ktoré definuje základnú výkonnostnú End-to-End metriku pre SIP telefóniu.

IMS klient BOGHE IMS/RCS generoval SIP správy ako SIP REGISTER a INVITE a dostával na ne odpovede. Merané boli časy odpovedí na jednotlivé správy, ako aj časy iných režijných správ ako ACK, BYE, 200 OK, 180 pri vytvorení a ukončení relácie s druhým IMS klientom. SIP provoz bol zachytávaný na klientských staniciach programom Wireshark a následne boli odčítavané potrebné časy. Tieto merania sa uskutočnili na IMS sieti, ktorá bola bez umelej záťaže a s umelou záťažou.

Časy boli zaznamenávané do tabuliek, z ktorých boli spravené grafy a vyrátané priemerné hodnoty jednotlivých parametrov a opäť vynesené do grafov. Meranie sa opakovalo 10-krát pre každú záťaž podobne ako v článku [13]. Práca nie je presne tým čo som mal vykonať a to výkonnostné testovanie IMS z pohľadu aplikačnej vrstvy (prezenčné služby). Dôvody uvádzam v kapitole 6.

8.1 Hardvérové a softvérové parametre serverov

8.1.1 Hardvér

4x Intel Core i5-2400S CPU@2.50 GHz with 6144k L3 cache, 8 GM RAM (DIMM 1333 MHz), 82574L Intel Gigabit Network Connection.

8.1.2 Operačný systém a softvér

GNU/Linux (Ubuntu 12.04 LTS, AMD64 architecture, kernel v3.2), softvérové implementácie CSCF serverov sú založené na SER (SIP Express Router) a HSS databáza je založená na FhoSS (FOKUS Home SubscriberServer) vytvorenom Fraunhofer FOKUS Institute.

8.1.3 Nastavovanie umelej záťaže

Umelá záťaž bola generovaná programom Lookbusy. Zaťažovaná bola pamäť RAM a CPU .

Záťaž bola generovaná v nasledujúcich kombináciách:

CPU 0 % RAM 25 %	CPU 100 % RAM 0 %
CPU 0 % RAM 50 %	CPU 100 % RAM 25 %
CPU 0 % RAM 75 %	CPU 100 % RAM 50 %
CPU 0 % RAM 95 %	CPU 100 % RAM 75 %
	CPU 100 % RAM 95 %

8.1.4 Nastavenie generátora

Ak chceme nastaviť záťaž napríklad CPU 90 %, 4 jadrá a RAM pamäť 3000MB, spravíme to nasledovným príkazom: lookbusy -c 90 -n 4 -m 3000mb.

8.1.5 Wireshark

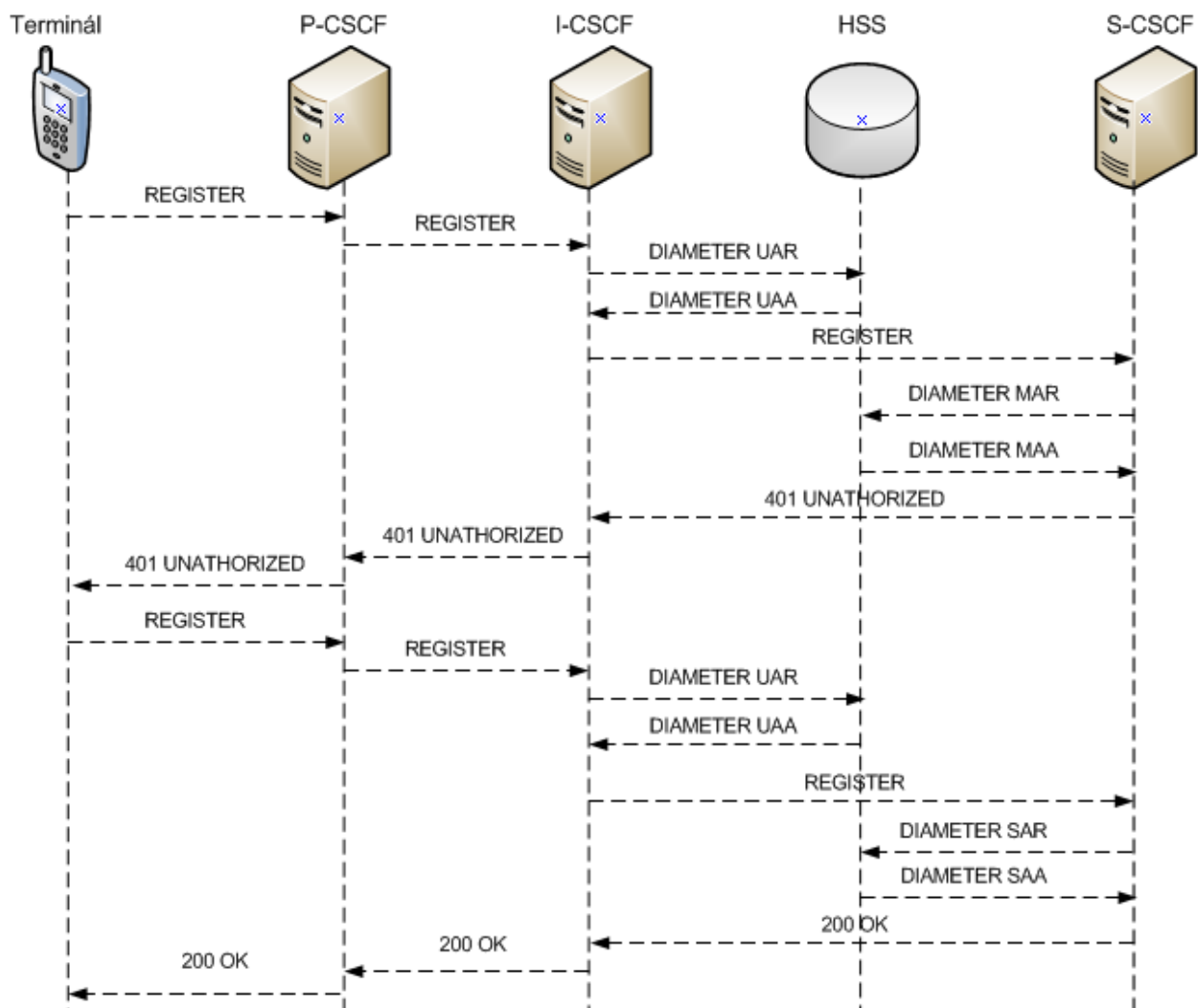
Na zachytávanie SIP provozu bol použitý program Wireshark.

8.2 Tok správ a porovnanie časov pri prihlasovaní a vytváraní relácie

8.2.1 Testované scenáre

a) Prihlásenie

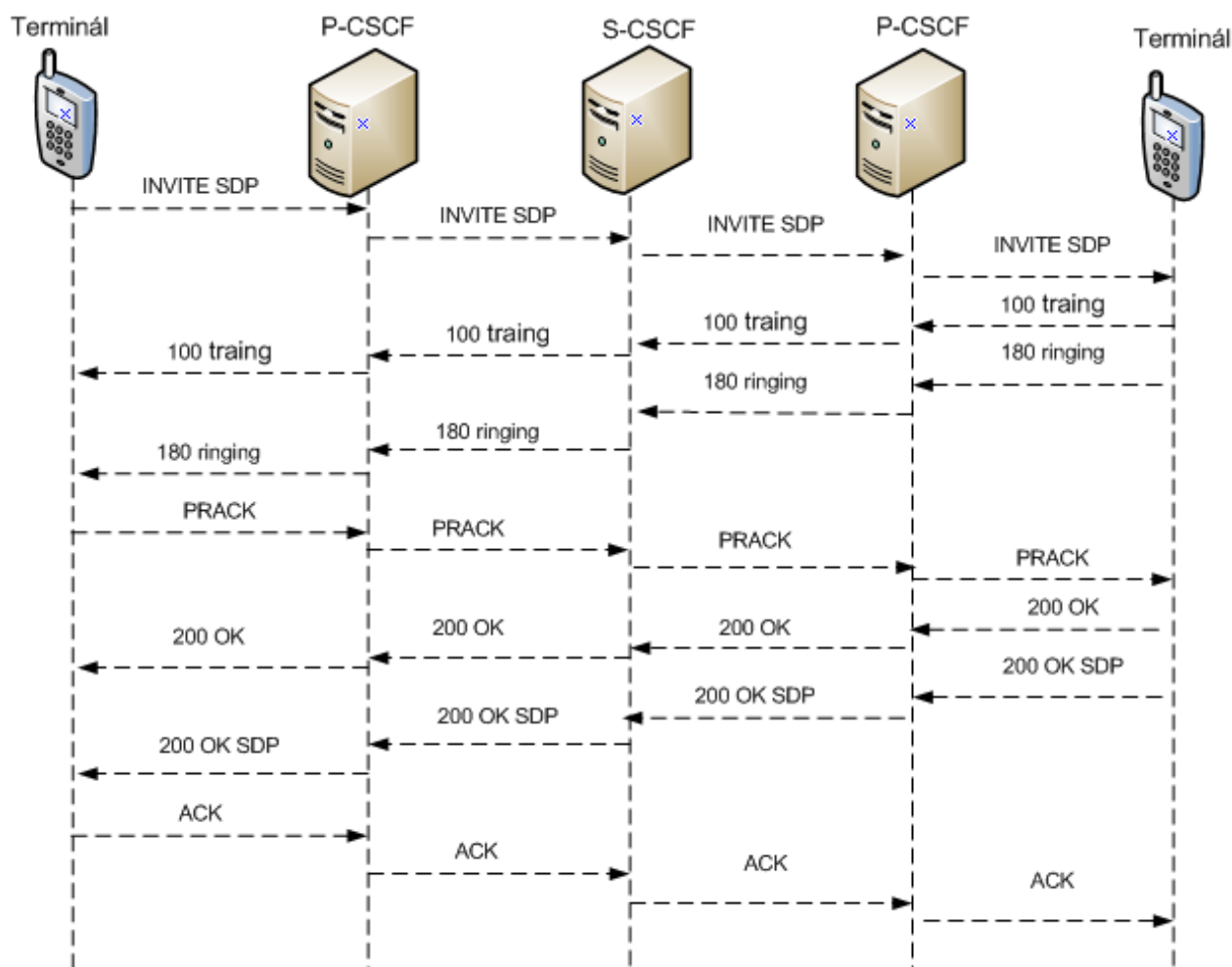
Na obrázku (Obr.č.32) vidíme tok správ pri prihlasovaní klienta do IMS siete, celá procedúra prihlasovania sa skladá z dvoch častí, jednej kedy nie sú odoslané autentifikačné údaje a druhý krát, kedy sú odoslané autentifikačné údaje. Komunikácia prebieha medzi všetkými CSCF servermi a HSS databázou. Značný vplyv na dobu prihlásenia má komunikácia cez Cx interface a diameter protokol medzi HSS databázou a S – CSCF a I – CSCF servermi. Preto je čas prihlásenia vyšší ako čas vytvorenia relácie.



Obrázok 32: Tok správ pri prihlasovaní

b) Vytvorenie relácie

Tok správ pri vytváraní relácie vidíme na obrázku (Obr.č.33). Tu nastáva komunikácia len medzi prvkami P – CSCF a S – CSCF a taktiež sa neodosielajú žiadne autentifikačné údaje.



Obrázok 33: Tok správ pri vytváraní relácie

8.3 Výsledky meraní

8.3.1 Internet Engineering Task Force (IETF) RFC 6076

Toto doporučení od organizácie IETF definuje základné testované parametre SIP End-to-End telefónie pre výpočet výkonnosti danej siete.

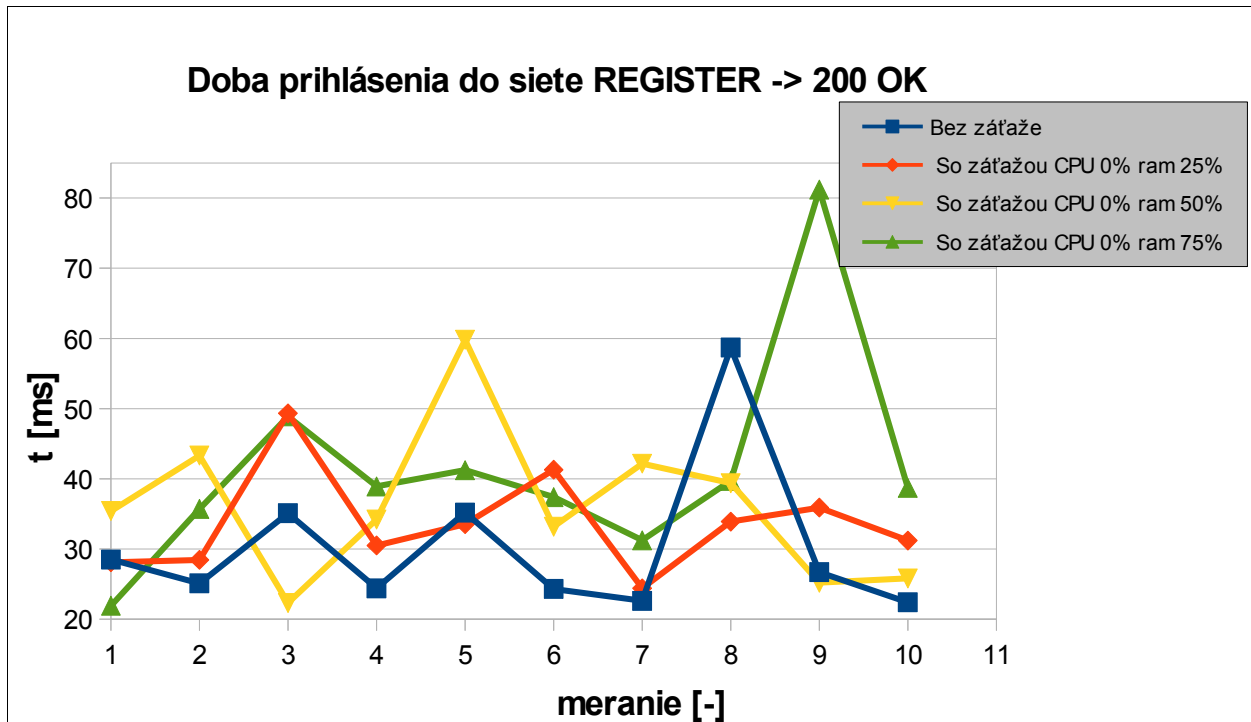
Definícia End-to-End hovorí o použití dvoch alebo viac koncových elementov zúčastnených pri vytváraní žiadosti, obdržaní žiadosti a odpovedaní na žiadosť. Toto zahŕňa prvky nevyhnutné pri vytváraní relácie medzi volajúcim (UAC) a volaným (UAS) a medziľahlými proxy servermi vrátane back-to-back user agents (B2BUAs) [21].

8.3.2 Registration Request Delay (RRD)

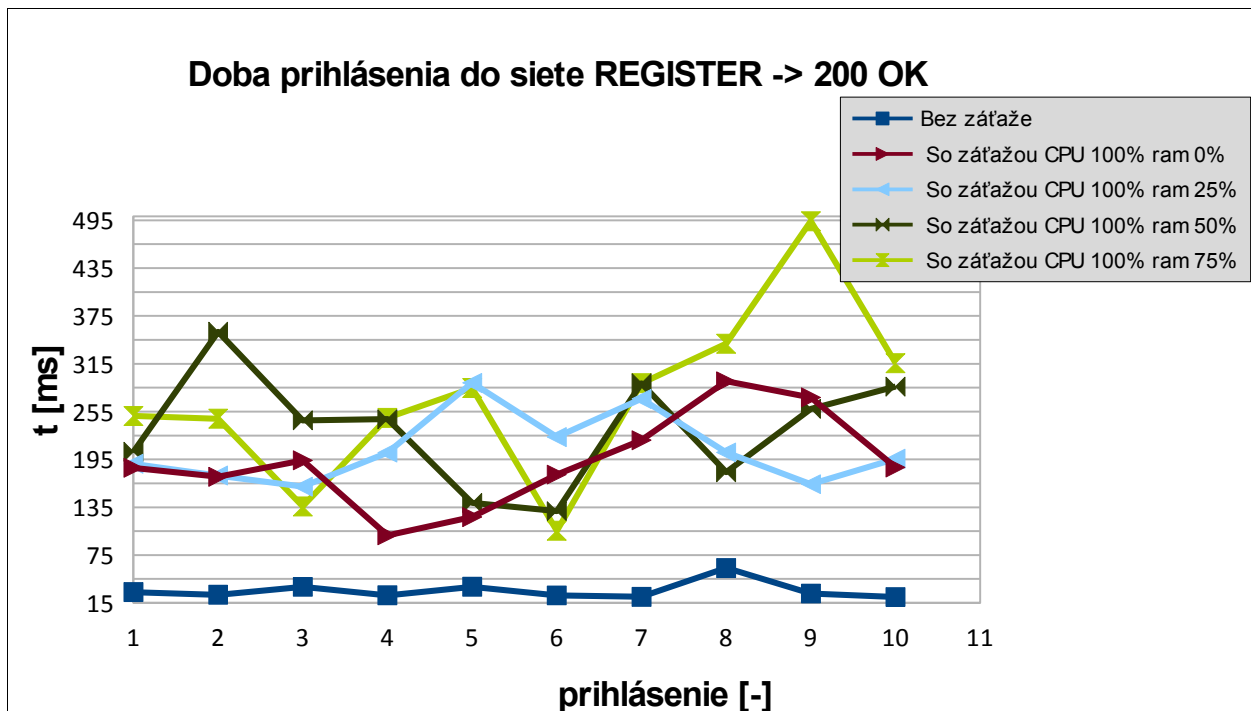
Tento parameter je doba prihlásenia užívateľa do IMS siete. Je to čas kladnej odpovede na SIP REGISTER vyslanej klientom.

Time	192.168.54.73	192.168.54.67
0,000	Request: REGISTER s	SIP: Request: REGISTER sip:utko.ims.network
0,008	Status: 401 Unautho	SIP: Status: 401 Unauthorized - Challenging the UE (0 bindings)
0,009	Request: REGISTER s	SIP: Request: REGISTER sip:utko.ims.network
0,021	Status: 200 OK - SA	SIP: Status: 200 OK - SAR succesful and registrar saved (2 bindings)

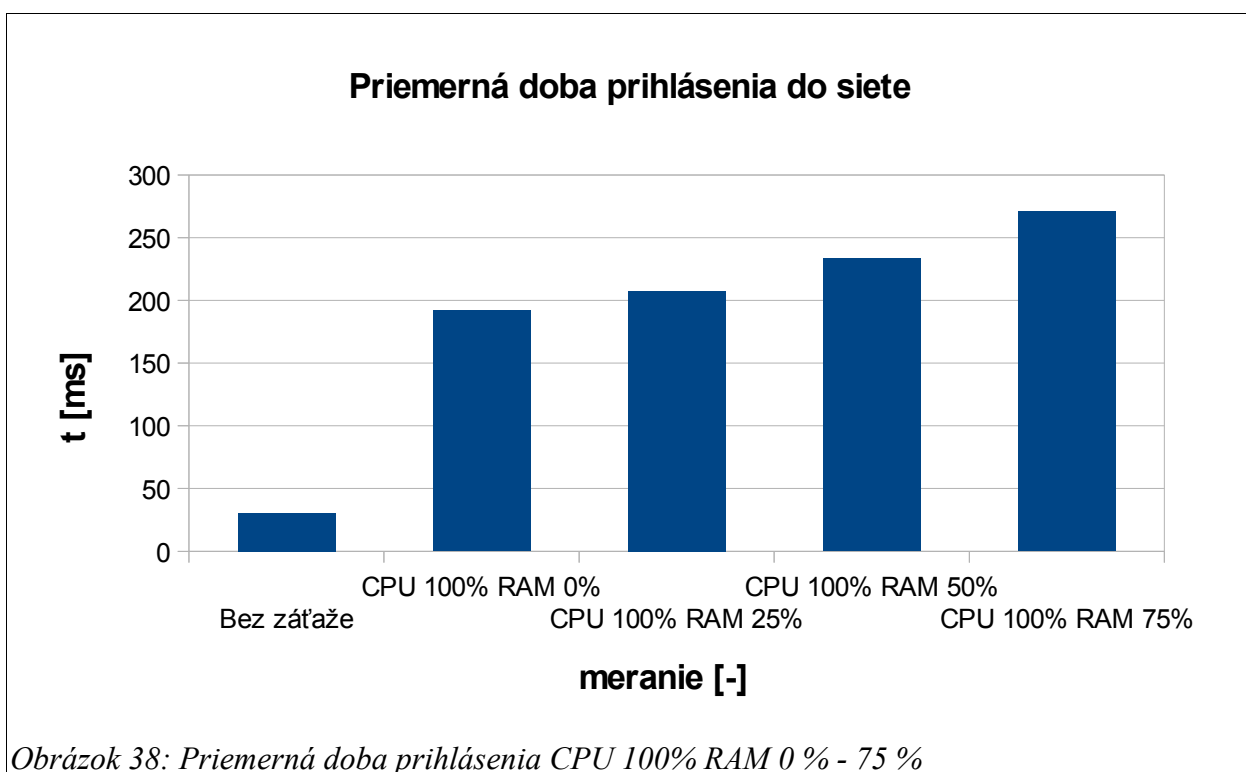
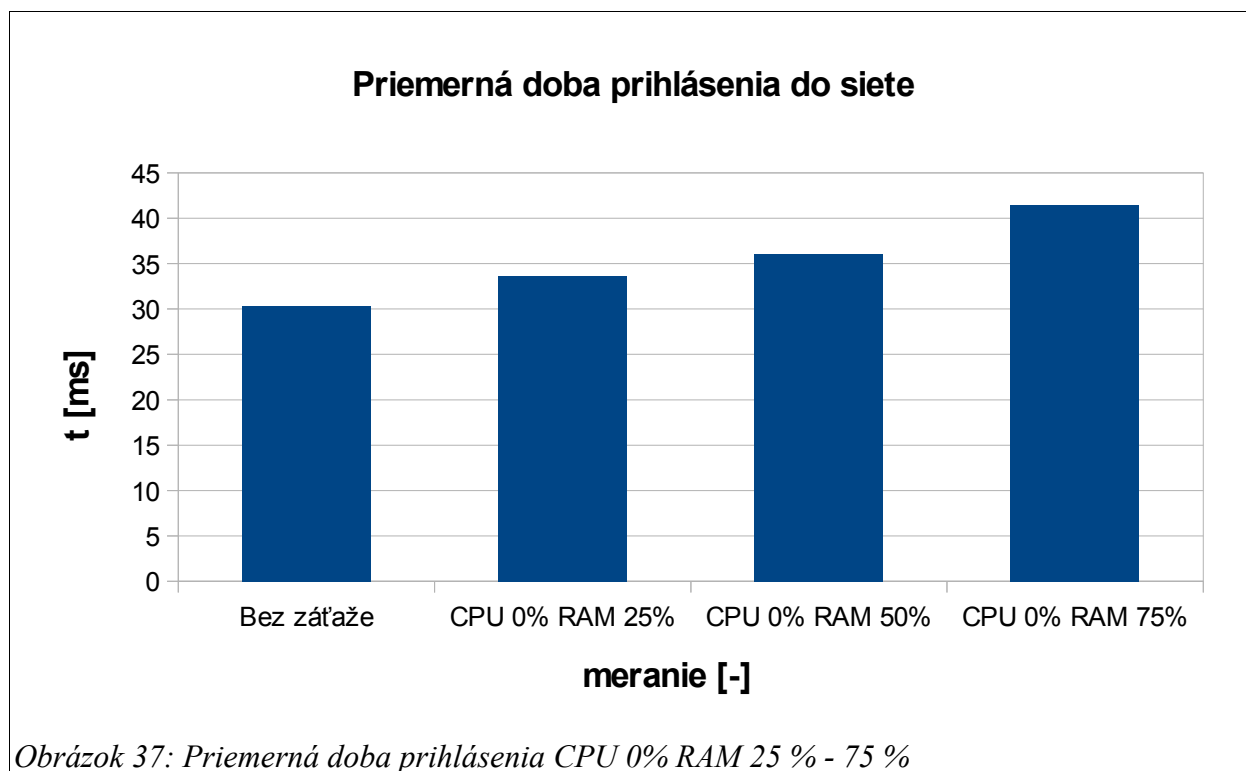
Obrázok 34: Flow graf, prihlásenie



Obrázok 35: Čas prihlásenia CPU 0 % RAM 25 % - 75 %



Obrázok 36: Čas prihlásenia CPU 100 % RAM 0 % - 75 %



Čas prihlásenia do siete je definovaný ako čas, ktorý uplynul medzi odoslaním žiadosti REGISTER klientom a prijatím spávy 200 OK od P – CSCF servera. Tento čas vyjadruje dobu prístupu užívateľa do IMS siete. Registračný proces zahŕňa obojstrannú autentifikáciu, kedy

UE overuje totožnosť IMS siete a IMS sieť zase totožnosť UE . Výsledky merania tejto metriky vidíme na grafoch Obr. č.(41-44). Priemerná doba prístupu do IMS bez umelej záťaže bola 30,3 ms. Väčšina prihlásení sa pohybovala okolo tejto hodnoty, avšak pri ôsmom meraní sa vyskytol nárast doby prihlásenia a to na 60 ms čo predstavuje 100 % nárast. Táto situácia bola spôsobená tým, že terminál odoslal 4 REGISTER žiadosti namiesto štandardných 2. Jednej bez autentifikačných údajov a druhú žiadosť, ktorá obsahuje potrebné údaje. Na obrázku (Obr. č.41) vidíme, že s postupným zaťažovaním operačnej pamäte CSCF serverov rástla aj doba prístupu do siete, pri záťaži 25 % to bolo 33,6 ms, pri 50 % 36 ms a pri 75 % 41,4 ms. Pri záťaži 75 % a 9 meranie vidíme opäť anomáliu v čase prihlásenia, ktorý bol 80 ms. Táto doba bola spôsobená tým, že server S – CSCF nestíhal spracovávať žiadosti prichádzajúce od P – CSCF. Výsledky zo záťaže RAM pamäte na 95 % nie sú zobrazené, pretože pri tejto záťaži server S – CSCF nedokázal komunikovať s databázou HSS, dochádzalo k interným chybám 5xx a výpadkom Cx rozhrania a klient sa nedokázal prihlásiť do siete. Na obrázku (Obr. č.42) vidíme graf doby prihlásenia, kedy bol procesor zaťažovaný na 100 % a s postupnou záťažou RAM pamäte. Pri 100 % CPU je doba prihlásenia oveľa väčšia. Priemerná doba prihlásenia pri záťaži 100 % CPU a 0 % RAM je 191,9 ms. Pri záťaži 25 % RAM je to 207,3 ms, pri 50 % 233,4 ms a pri 75 % 270,5 ms. Pri záťaži RAM 75 % a CPU 100 % pri deviatom meraní je vidieť maximum doby prihlásenia 498 ms a následný pokles na 315 ms, to bude pravdepodobne dané technológiou procesorov v CSCF serveroch. Tieto procesory, ak sú maximálne zaťažované, umožňujú dynamické pretaktovanie a tak zvýšenie svojho výkonu na krátky okamih, to by vysvetľovalo značný rozsah doby prihlásenia pri 100 % záťaži procesora. Lepší prehľad percentuálneho nárastu doby spracovania žiadosti o prihlásenie vidíme v tabuľke 5 a 6.

Tabuľka 5: Priemerná doba prihlásenia CPU 100 % RAM 0 % - 75 %

		Bez záťaže			
		So záťažou			
		CPU 100% RAM 0%	CPU 100% RAM 25%	CPU 100% RAM 50%	CPU 100% RAM 75%
Priemerná doba prihlásenia [ms]	33,3	191,9	207,7	233,4	270,9
Percentuálny nárast [%]	0	476,2	523,7	600,9	713,51

Tabuľka 6: Priemerná doba prihlásenia CPU 0% RAM 25 % - 75 %

	Bez zátáže	So zátážou		
		CPU 0 % RAM 25%	CPU 0% RAM 50%	CPU 0% RAM 75%
Priemerná doba prihlásenia [ms]	33,3	33,6	36	41,4
Percentuálny nárast [%]	0	0,9	8,1	24,3

8.3.3 Ineffective registration attempts (IRAs)

Táto metrika reprezentuje schopnosť, resp. neschopnosť P-CSCF obdržať a vyhodnotiť SIP REGISTER žiadosť od klienta. Je rátaná v percentách a to nasledovným spôsobom:

$$IRA = \frac{IRAs}{\text{celkový počet SIP REGISTER}} * 100 [\%] [13].$$

Neúspešná registrácia je definovaná ako chybová odpoveď na počiatočnú REGISTER správu.

Chybovými odpoveďami sú definované správy: 4XX (okrem 401, 402, a 407 non-failure challenge response codes), 5XX, alebo 6XX správou. A vypršaním časovača Timer F Expiring .

Je ekvivalentom ku KPI pre prihlásenie.

```

|Time      | 192.168.54.73 | 192.168.54.67 |
|-----|-----|-----|
|12,309    | Request: REGISTER s | SIP: Request: REGISTER sip:utko.ims.network
| | (53212) -----> (4060) |
|12,808    | Request: REGISTER s | SIP: Request: REGISTER sip:utko.ims.network
| | (53212) -----> (4060) |
|13,808    | Request: REGISTER s | SIP: Request: REGISTER sip:utko.ims.network
| | (53212) -----> (4060) |
|15,808    | Request: REGISTER s | SIP: Request: REGISTER sip:utko.ims.network
| | (53212) -----> (4060) |
|19,808    | Request: REGISTER s | SIP: Request: REGISTER sip:utko.ims.network
| | (53212) -----> (4060) |
|10,500    | Status: 480 Tempora | SIP: Status: 480 Temporarily Unavailable - Diameter Cx interface failed
| | (53212) <----- (4060) |

```

Obrázok 39: Flow graf, IRA

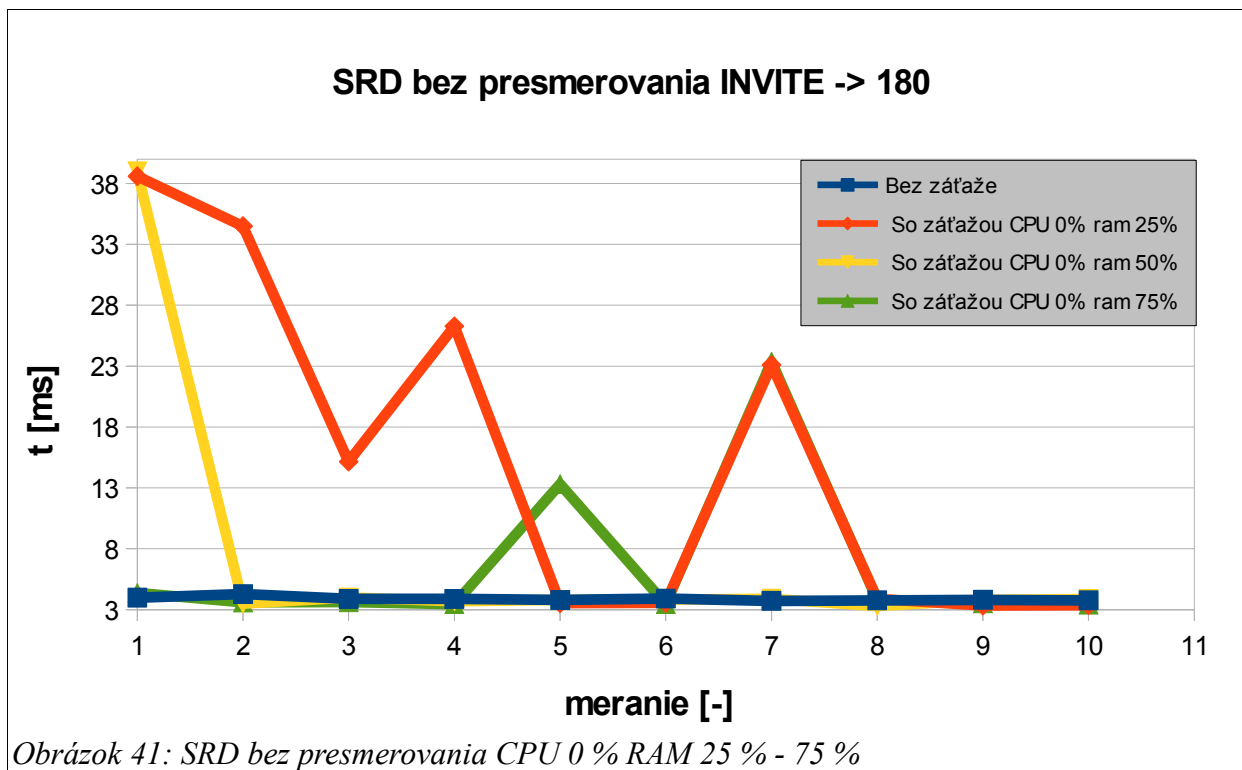
8.3.4 Session request delay bez presmerovania (SRD)

Táto metrika vyjadruje čas odpovede na správu INVITE, žiadosť klienta o vytvorenie relácie (hovoru alebo video-hovoru). Môže byť meraná za použitia presmerovania redirekt serverom alebo nie. V mojom prípade som nepoužil redirekt server [21].

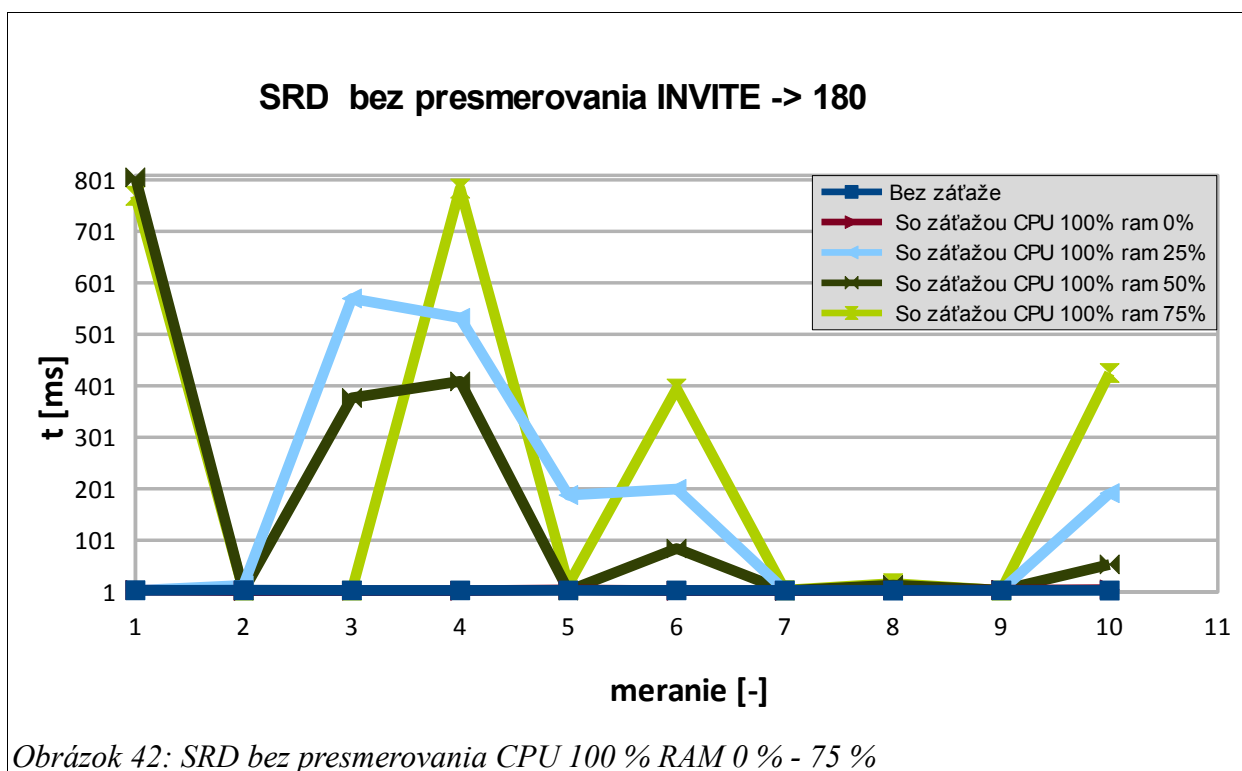
Čas je meraný len v prípade úspešnej odpovede – 180 Ringing, medzi neúspešné odpovede patria správy: 4XX (okrem 401, 402, a 407 non-failure challenge response codes), 5XX, alebo 6XX správ [21].

Time	192.168.54.72	192.168.54.67	
6,983	Request: INVITE sip		SIP/SDP: Request: INVITE sip: bob@utko.ims.network , with session description
	(59829) ----->	(4060)	
6,983	Status: 100 trying		SIP: Status: 100 trying -- your call is important to us
	(59829) <-----	(4060)	
6,987	Status: 180 Ringing		SIP: Status: 180 Ringing
	(59829) <-----	(4060)	

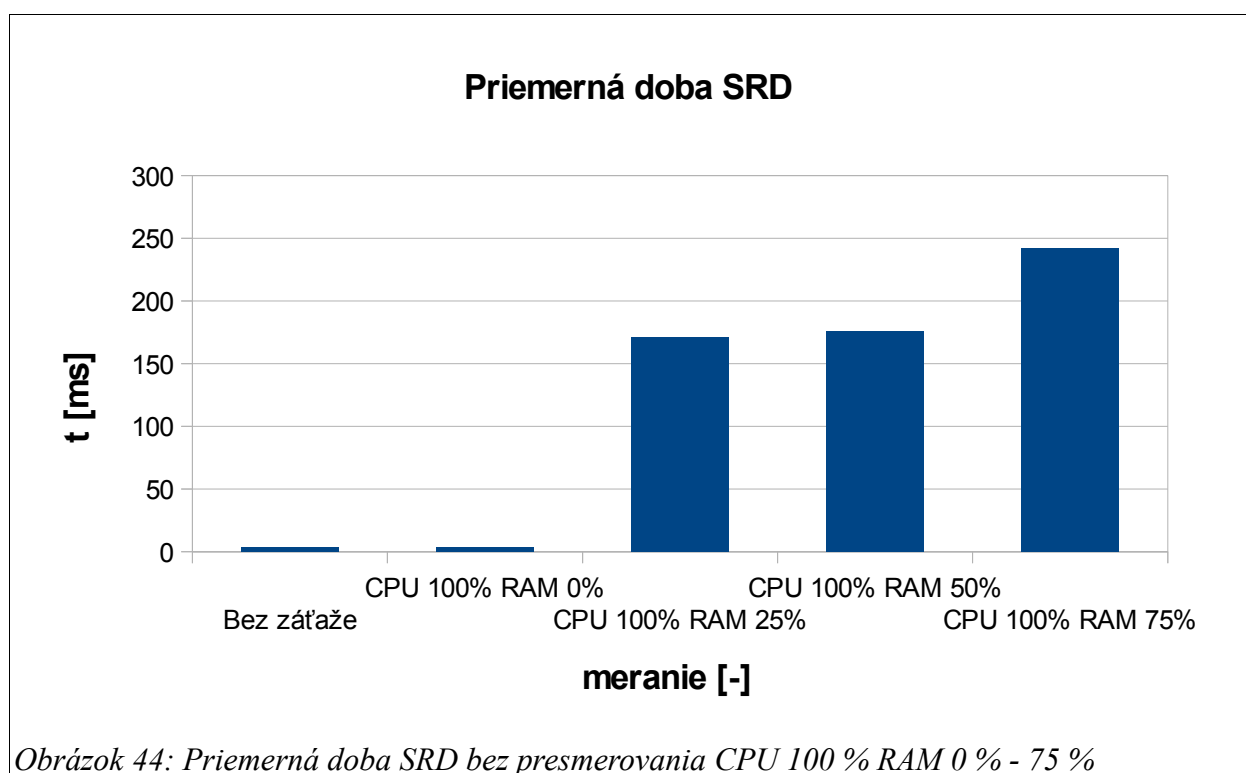
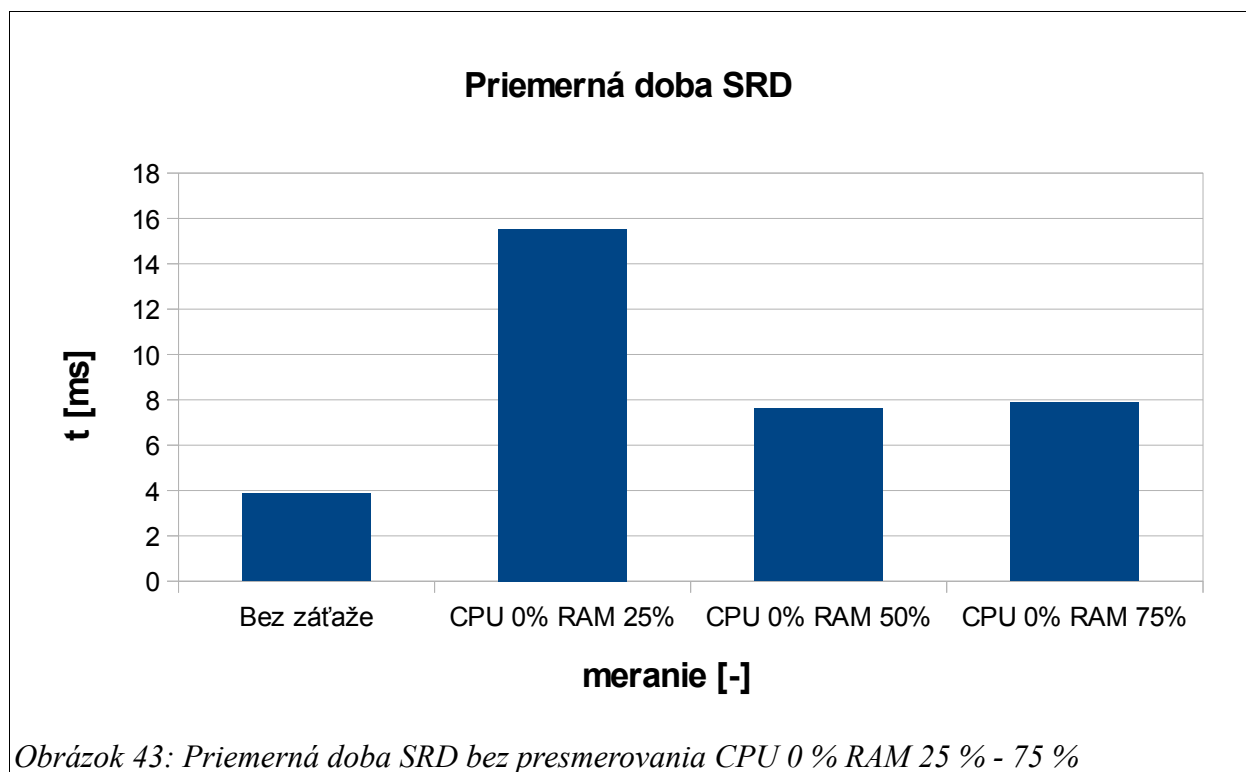
Obrázok 40: Flow graf, SRD bez presmerovania



Obrázok 41: SRD bez presmerovania CPU 0 % RAM 25 % - 75 %



Obrázok 42: SRD bez presmerovania CPU 100 % RAM 0 % - 75 %



S touto metrikou sa môžeme stretnúť aj ako s Initial ringing time, predstavuje čas, ktorý uplynul medzi odoslaním správy INVITE a prijatím správy 180 ringing. Prijatiu tejto správy predchádza správa 100 traying. Priemerná doba bez záťaže je 3,87 ms a maximálna priemerná doba je pri záťaži CPU 100 % a RAM 75 % 242,2 ms, čo predstavuje rapidný nárast. Priemerná doba pri

zátäži CPU 0 % a RAM 25 % je 15,6 ms a pri RAM 50 % a RAM 75 % je 7 ms a 8 ms, táto chyba je daná nepresnosťou merania. Ako vidíme v grafoch, táto doba rapídne stúpla pri maximálnej záťaži procesora a operačnej pamäte až na 800 ms kedy pri 0 % záťaži CPU a RAM 75 % dosahuje len 39 ms. Podobné správanie siete je vidieť aj pri dobe prihlásenia. Pri maximálnej záťaži je priemerný čas porovnateľný s priemerným časom pri záťaži CPU 100 % a RAM 50 % aj keď pri relácií sa využívajú len servery P – CSCF a S – CSCF bez autentifikácie a sú to všetky CSCF servery a HSS databáza, teda logicky vyplýva, že čas prihlásenia by mal byť oveľa väčší. Avšak to, že čas je porovnateľný môže byť dané inicializáciou RTP protokolu a samozrejme nepresnosťami experimentu. Na túto metriku mala veľký vplyv záťaž procesora.

Tabuľka 7: Priemerná doba SRD bez presmerovania CPU 0 % RAM 25 % - 75 %

Bez záťaže		So záťažou			
		CPU 100% RAM 0%	CPU 100% RAM 25%	CPU 100% RAM 50%	CPU 100% RAM 75%
Priemerná doba SRD[ms]	3,87	3,9	171,3	176,1	242,2
Percentuálny nárast [%]	0	0,77	4326	4450	6158

Tabuľka 8: Priemerná doba SRD bez presmerovania CPU 100 % RAM 0 % - 75 %

Bez záťaže		So záťažou		
		CPU 0 % RAM 25%	CPU 0% RAM 50%	CPU 0% RAM 75%
Priemerná doba SRD[ms]	3,87	15,53	7,2	6,5
Percentuálny nárast [%]	0	301,2	86	67,9

8.3.5 Ineffective session attempts (ISAs)

Táto metrika definuje podiel odpovedí na správu INVITE asociovaných so správami 408,500, 503, 504 k celkovému počtu INVITE žiadostí. Odpovede typu 408, 500, 503, 504 sa vyskytli pri preťažení serverov CSCF [21].

Time	192.168.54.73	192.168.54.67
10,000	Request: INVITE sip	SIP/SDP: Request: INVITE sip: bob@utko.ims.network , with session description
10,499	(53135) -----> (4060)	SIP/SDP: Request: INVITE sip: bob@utko.ims.network , with session description
11,499	Request: INVITE sip	SIP/SDP: Request: INVITE sip: bob@utko.ims.network , with session description
11,913	(53135) -----> (4060)	SIP: Status: 100 trying -- your call is important to us
13,552	Status: 100 trying	SIP: Status: 100 trying -- your call is important to us
	(53135) -----> (4060)	
	Status: 500 I'm ter	SIP: Status: 500 I'm terribly sorry, server error occurred (1/TM)

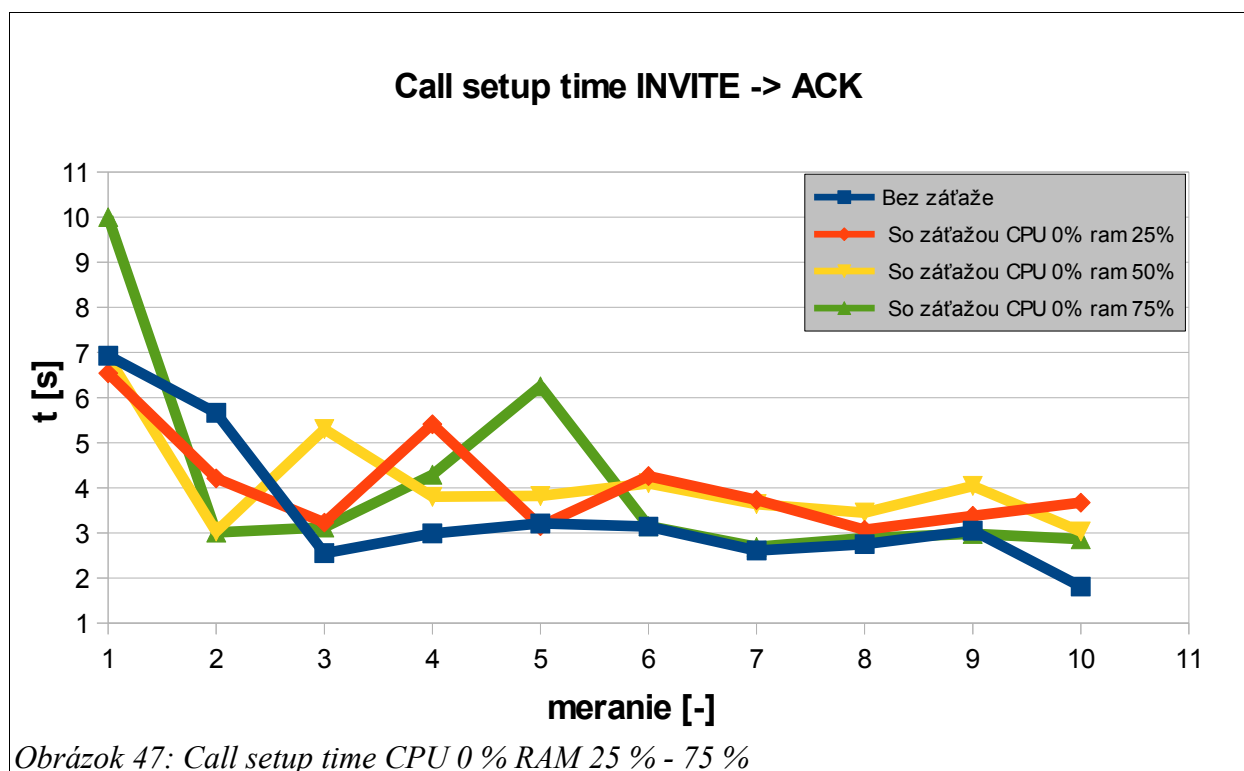
Obrázok 45: Flow graf, ISA

8.3.6 Call setup time

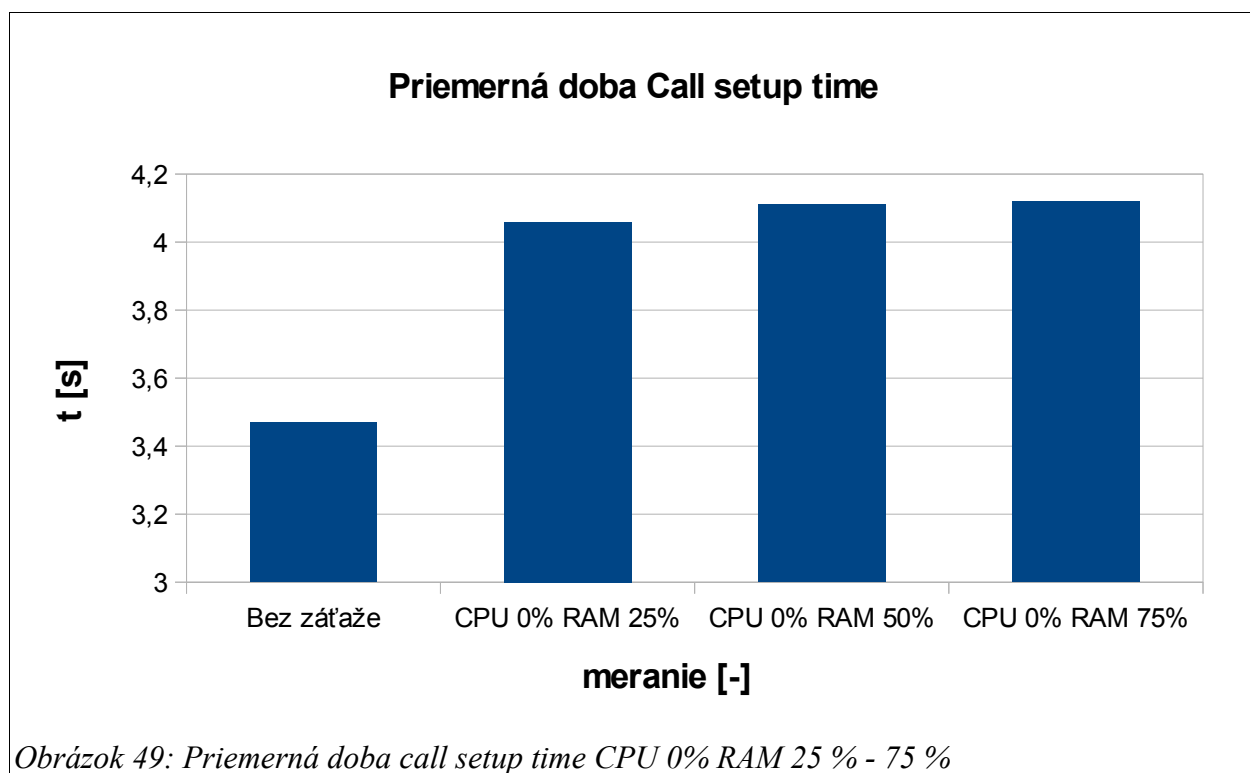
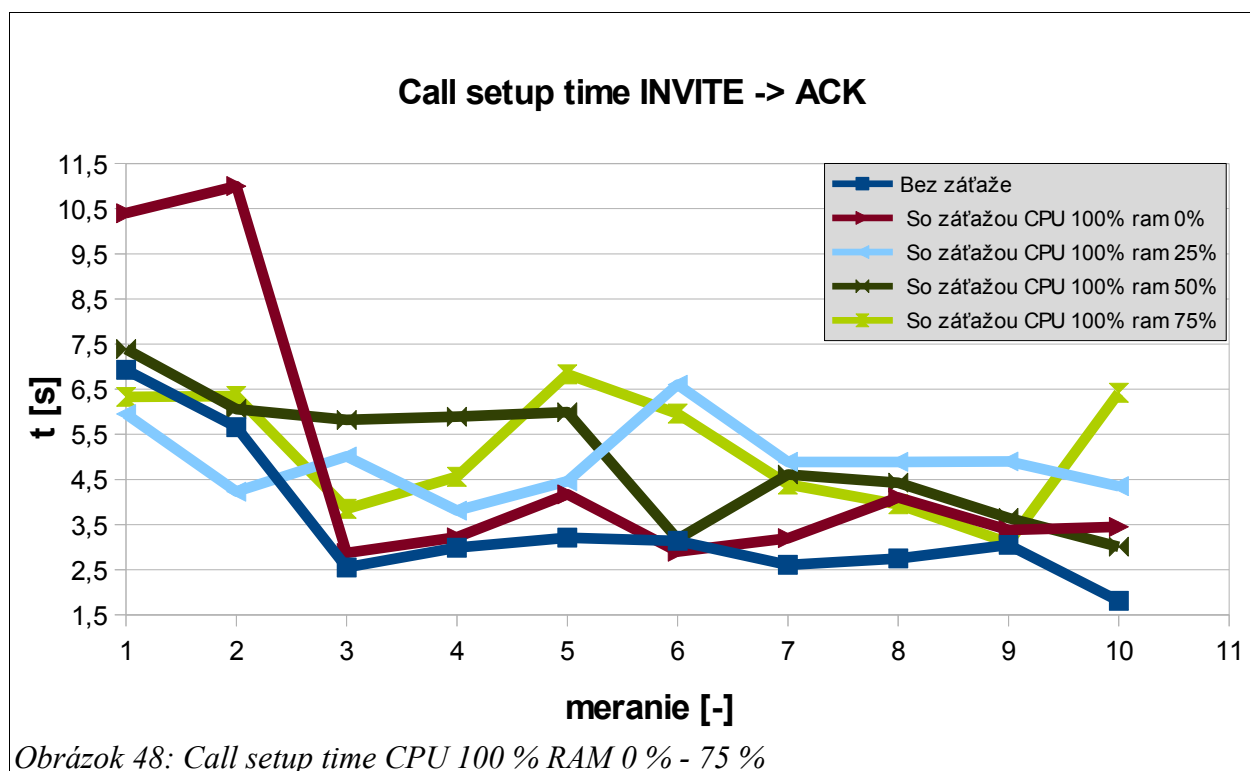
Táto metrika vyjadruje dobu, ktorá je definovaná ako čas medzi odoslaním žiadosti INVITE klientom a prijatím správy ACK. V tomto prípade je ACK potvrdením na správu PRACK, ktorú odosiela volajúci terminál a je potvrdením na správu 180 ringing.

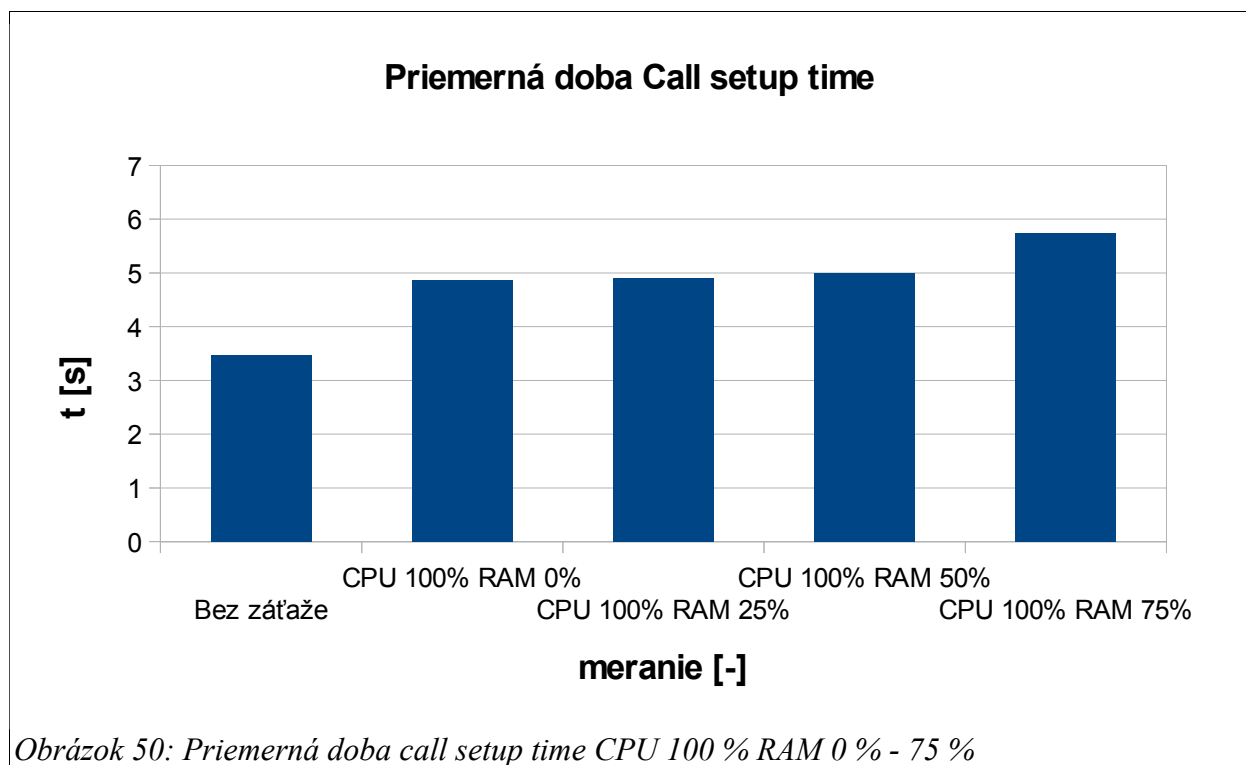
Time	192.168.54.72	192.168.54.67
10,000	Request: INVITE sip	SIP/SDP: Request: INVITE sip: bob@utko.ims.network , with session description
10,000	(59829) -----> (4060)	SIP: Status: 100 trying -- your call is important to us
10,004	Status: 100 trying	SIP: Status: 100 trying -- your call is important to us
10,004	(59829) -----> (4060)	SIP: Status: 180 Ringing
10,004	Status: 180 Ringing	SIP: Status: 180 Ringing
10,004	(59829) -----> (4060)	SIP: Request: PRACK sip: bob@192.168.54.73:49516;transport=udp
10,006	Request: PRACK sip:	SIP: Status: 200 OK
10,006	(59829) -----> (4060)	SIP: Status: 200 OK
12,910	Status: 200 OK, wit	SIP/SDP: Status: 200 OK, with session description
12,993	(59829) -----> (4060)	SIP: Request: ACK sip: bob@192.168.54.73:49516;transport=udp
	Request: ACK sip:bo	
	(59829) -----> (4060)	

Obrázok 46: Flow graf, call seetup time



Obrázok 47: Call setup time CPU 0 % RAM 25 % - 75 %





Čas predstavuje dobu zdvihnutia hovoru volaným užívateľom, čiže závisí od toho, ako rýchlo som na druhom počítači zdvihol prichádzajúci hovor. Všetky anomálie v grafoch sú teda spôsobené tým, ako bolo meranie uskutočnené. Avšak vplyv zaťaženia na tento čas je, ale nie je výrazný, pretože pred zdvihnutím hovoru musí prebehnúť výmena správ 100 traying, 180 ringing a PRACK, ktoré nie sú ovplyvnené tým, kedy bude zdvihnutý hovor, prebiehajú automaticky. Servery ich musia spracovať.

Tabuľka 9: Priemerná doba call setup time CPU 100 % RAM 0 % - 75 %

	Bez záťaže	So záťažou			
		CPU 100% RAM 0%	CPU 100% RAM 25%	CPU 100% RAM 50%	CPU 100% RAM 75%
Priemerná doba Call setup time[s]	3,47	4,86	4,9	5	5,17
Percentuálny nárast [%]	0	40	41	44	48,9

Tabuľka 10: Priemerná doba call setup time CPU 0% RAM 25 % - 75 %

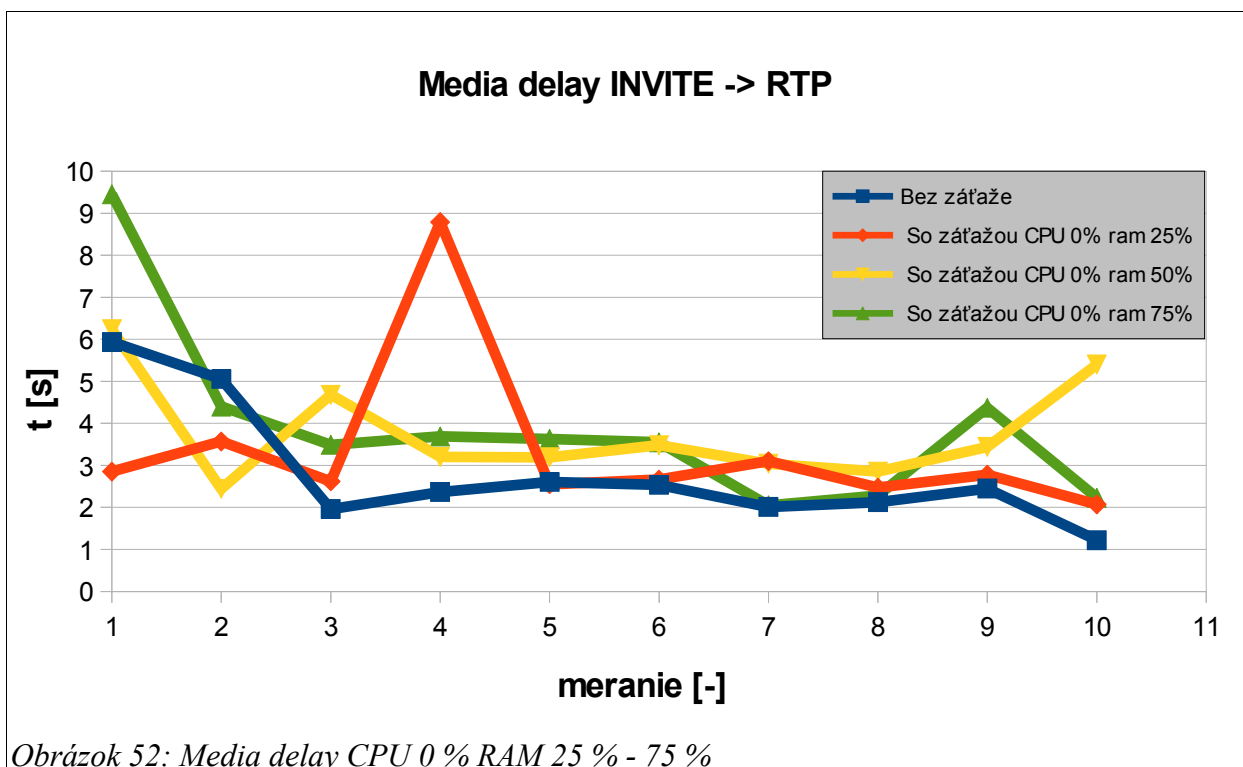
	Bez záťaže	So záťažou		
		CPU 0 % RAM 25%	CPU 0% RAM 50%	CPU 0% RAM 75%
Priemerná doba Call setup time[s]	3,47	4	4,11	4,12
Percentuálny nárast [%]	0	15,2	18,4	18,7

8.3.7 Media Delay

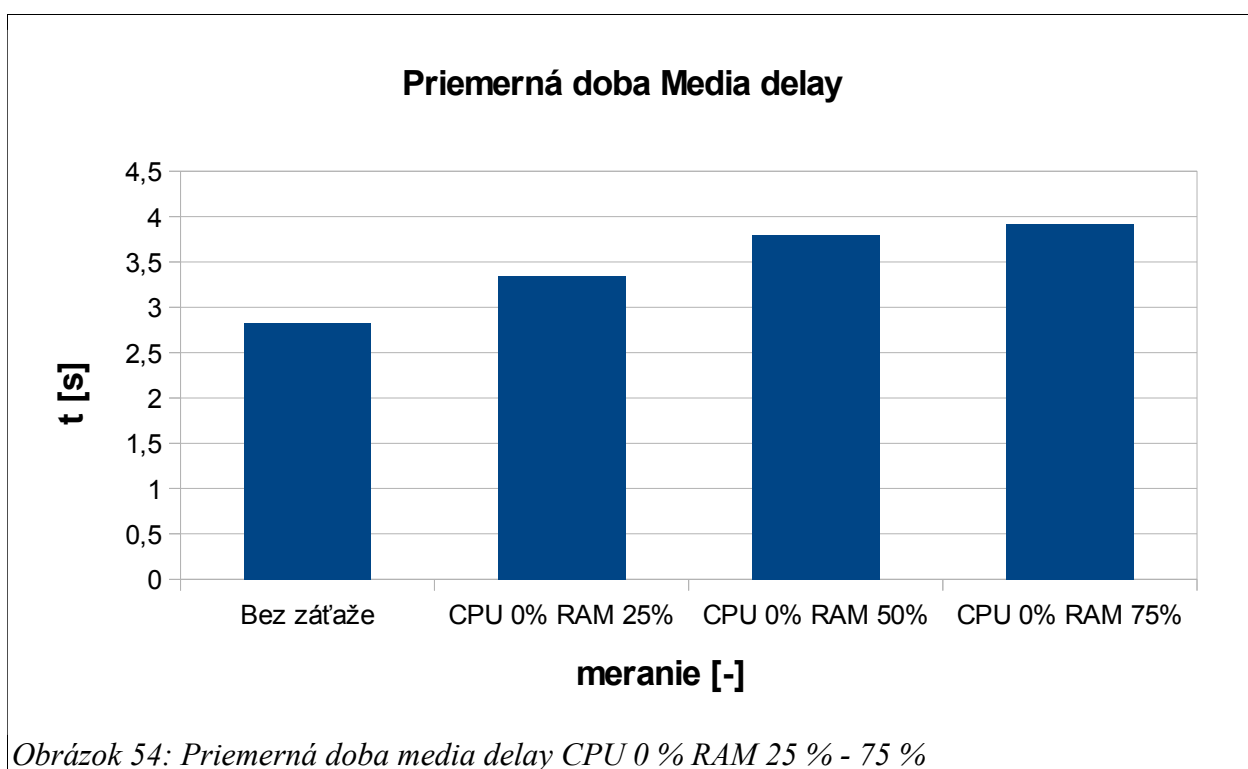
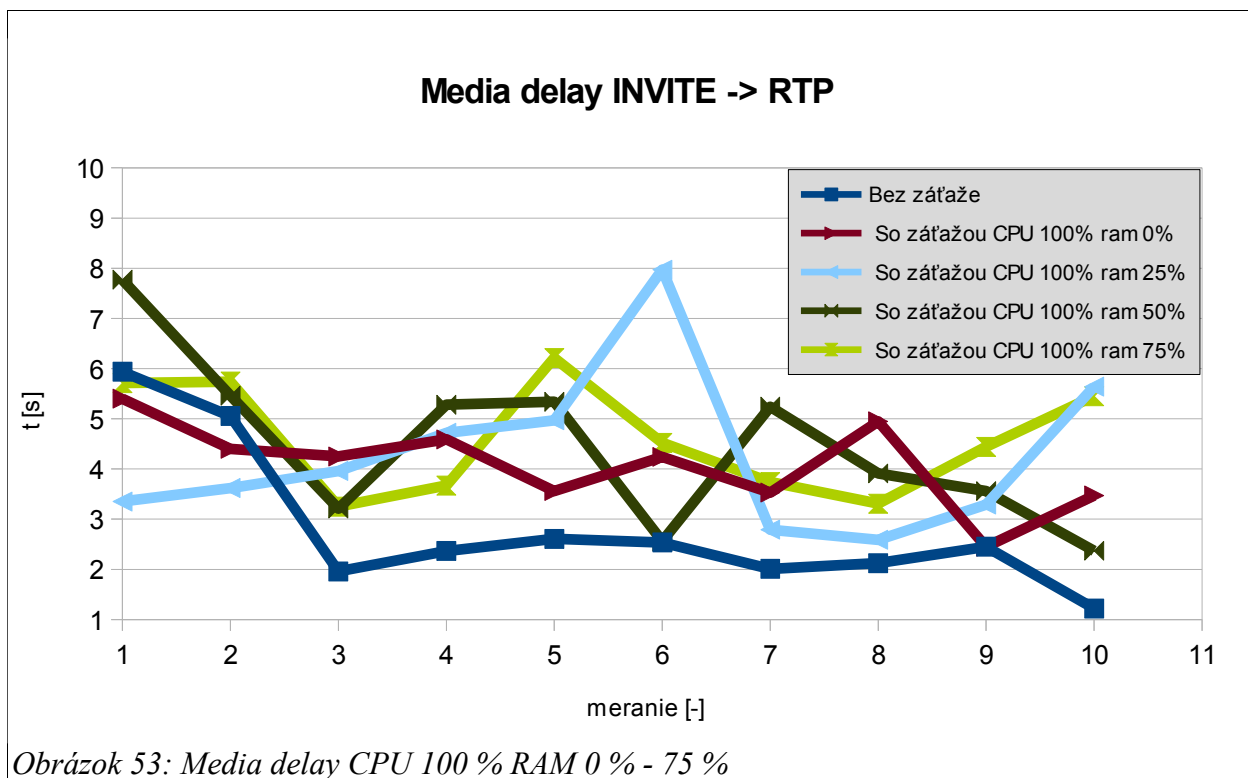
Media delay vyjadruje čas medzi odoslaním žiadosti o vytvorenie relácie INVITE a prijatím prvého RTP paketu.

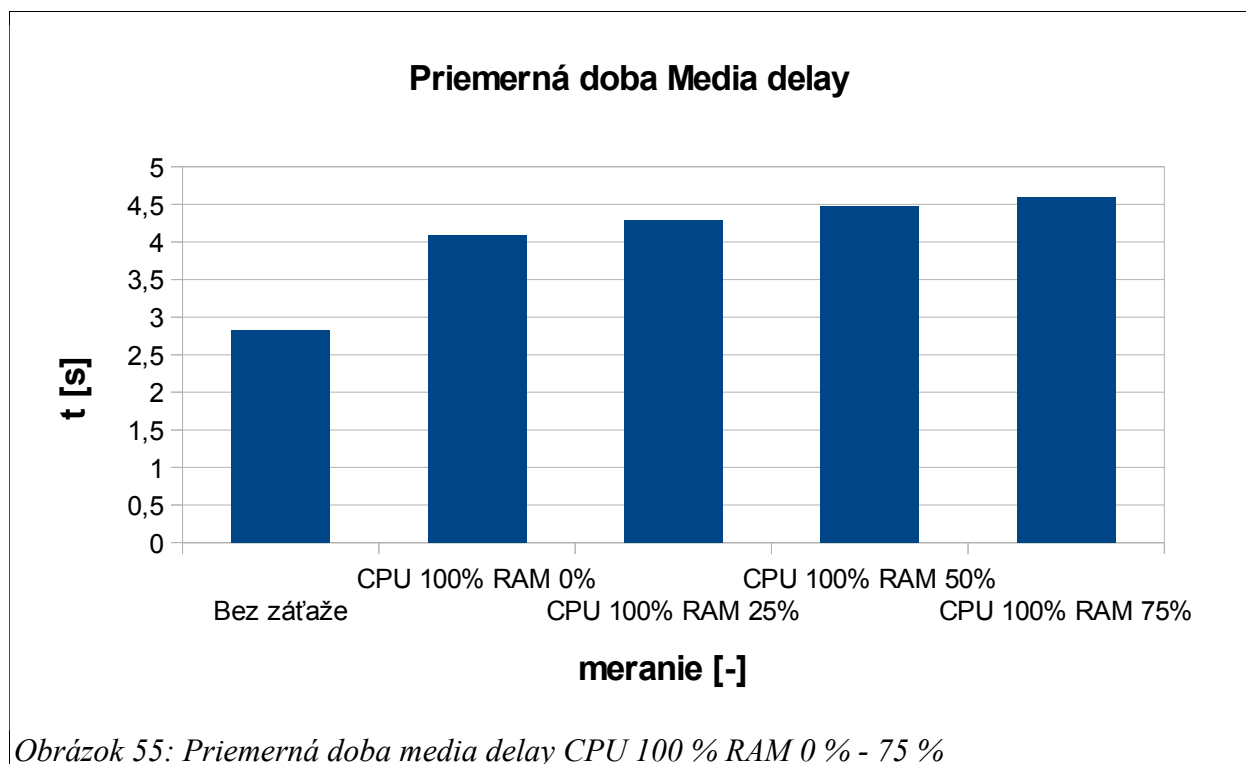
Time	192.168.54.72	192.168.54.67	192.168.54.73	
0,000	Request: INVITE sip			SIP/SDP: Request: INVITE sip: bob@utko.ims.network , with session description
0,000	(59829) -----> (4060)			
0,000	Status: 100 trying			SIP: Status: 100 trying -- your call is important to us
0,004	(59829) <----- (4060)			
0,004	Status: 180 Ringing			SIP: Status: 180 Ringing
0,004	(59829) <----- (4060)			
0,004	Request: PRACK sip:			SIP: Request: PRACK sip: bob@192.168.54.73 :49516;transport=udp
0,006	(59829) -----> (4060)			
0,006	Status: 200 OK			SIP: Status: 200 OK
0,006	(59829) <----- (4060)			
2,368	PT=Reserved for RTC			RTP: PT=Reserved for RTCP conflict avoidance, SSRC=0x81C&000F, Seq=1, Time=1
2,368	(14990) -----> (7775)			

Obrázok 51: Flow graf, media delay



Obrázok 52: Media delay CPU 0 % RAM 25 % - 75 %





Prvé RTP/RTCP pakety slúžia na rezerváciu potrebnej šírky pásma pre vytváranú reláciu. Prvému RTP paketu predchádzajú správy 100 traying, 180 ringing, PRACK a 200 OK. Čas je taktiež ovplyvnený dobou, kedy som zdvihol hovor na druhom počítači. Rovnako je aj čiastočne ovplyvnená záťažou, pretože taktiež predchádza výmena správ, ktoré sú zasielané automaticky a tak neovplyvnené týmto nedostatkom pri meraní.

Tabuľka 11: Priemerná doba media delay CPU 100 % RAM 0 % - 75 %

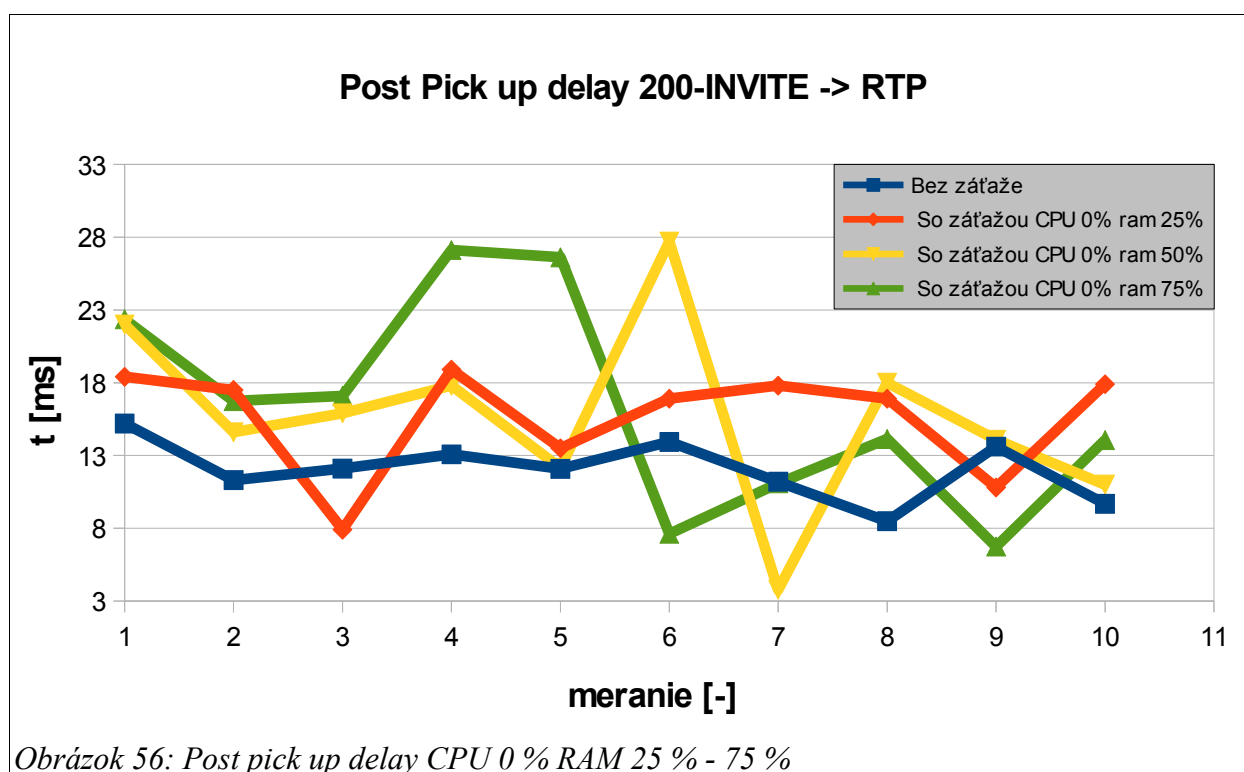
	Bez záťaže	So záťažou			
		CPU 100% RAM 0%	CPU 100% RAM 25%	CPU 100% RAM 50%	CPU 100% RAM 75%
Priemerná doba Media delay[s]	2,8	4	4,29	4,47	4,6
Percentuálny nárast [%]	0	42,8	53,2	59,6	64,2

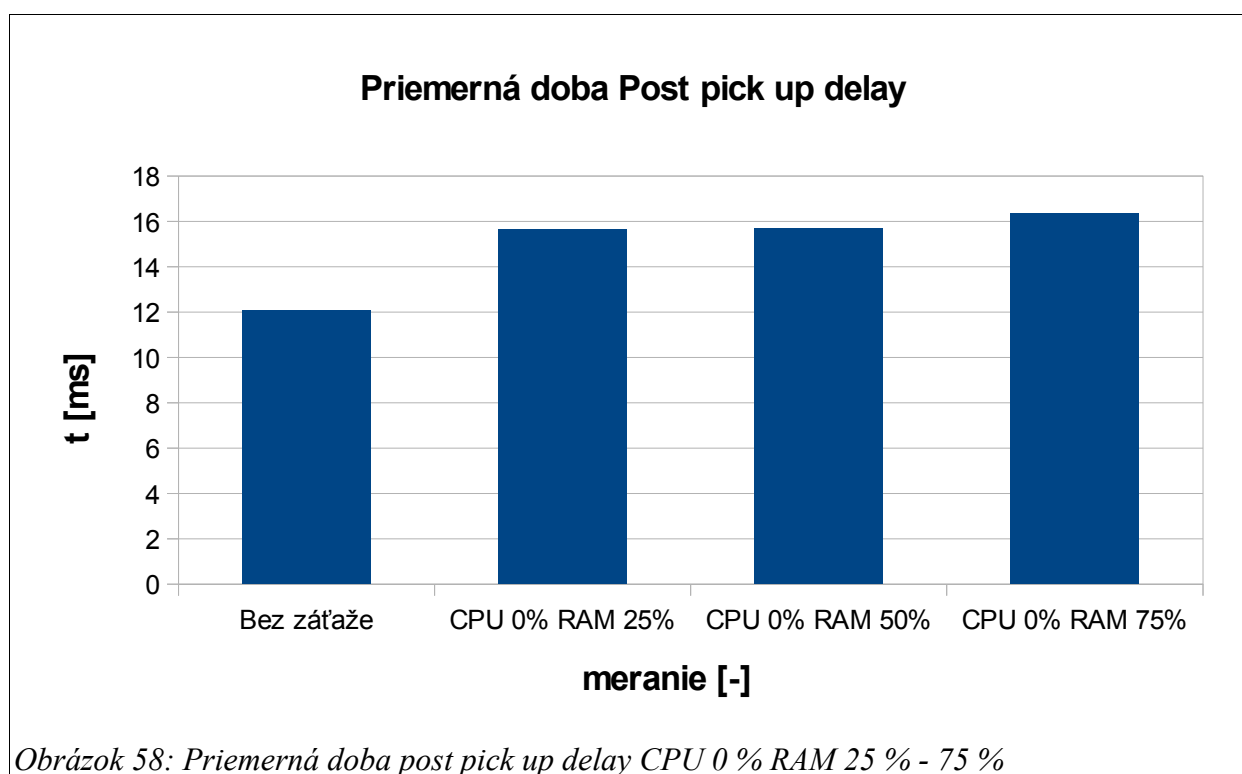
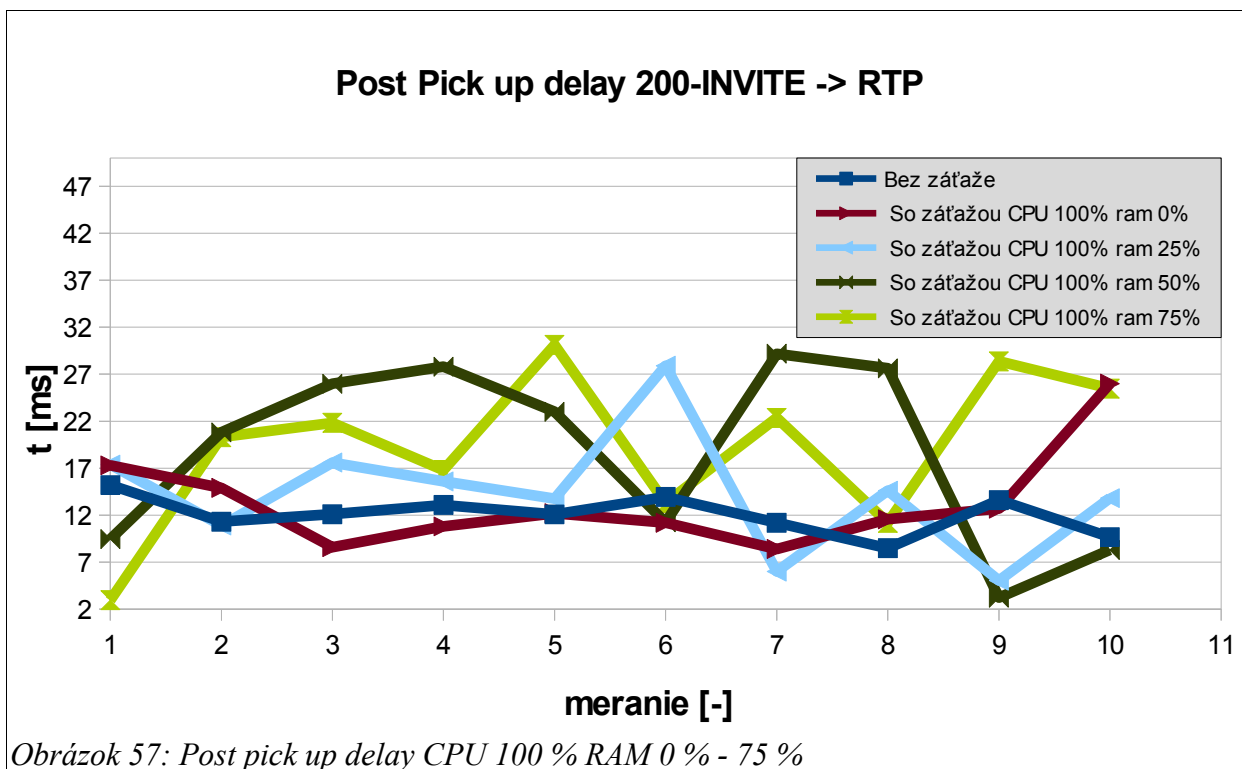
Tabuľka 12: Priemerná doba media delay CPU 0 % RAM 25 % - 75 %

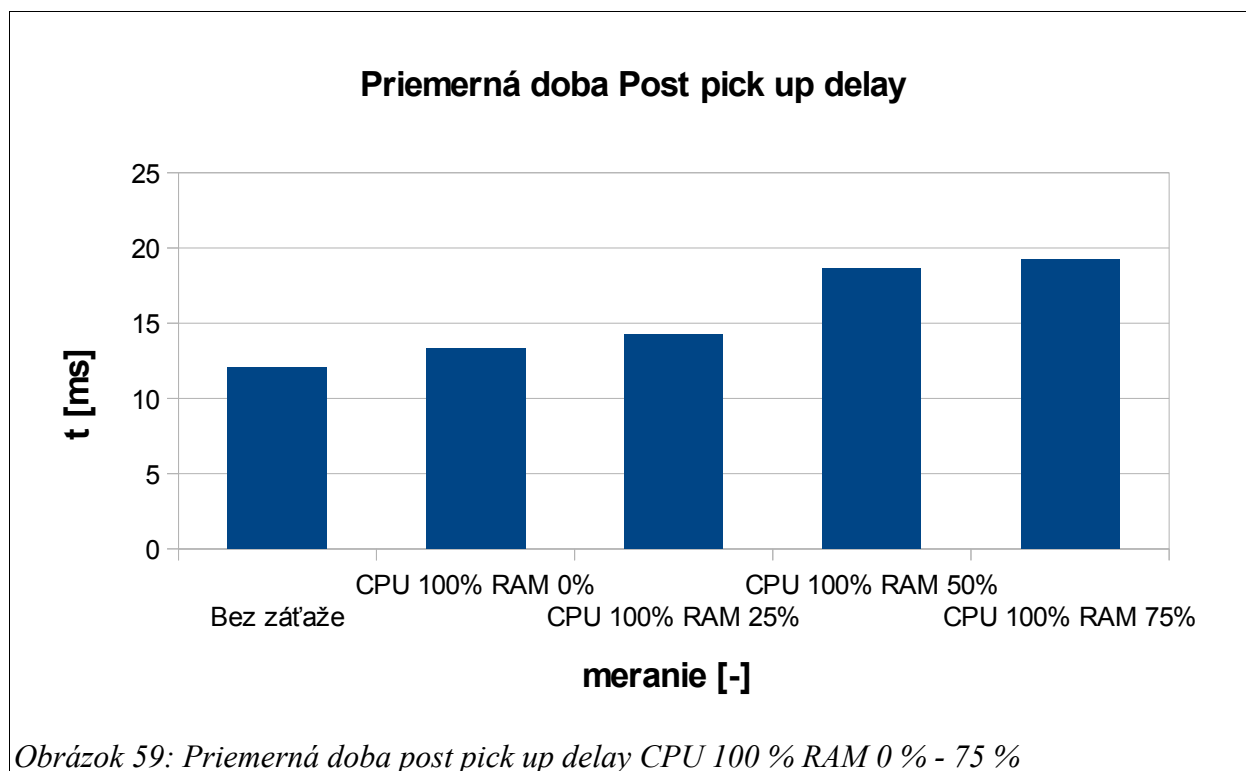
	Bez záťaže	So záťažou		
		CPU 0 % RAM 25%	CPU 0% RAM 50%	CPU 0% RAM 75%
Priemerná doba Media delay [s]	2,8	3,34	3,7	3,9
Percentuálny nárast [%]	0	19,2	32,1	39,2

8.3.8 Post Pick up delay

Post pick up delay je čas definovaný ako doba medzi potvrdením 200 OK SDP na správu INVITE with SDP a prvým RTP paketom.







Táto metrika nie je ovplyvnená tým, kedy zdvihnem prichádzajúci hovor, výmena správ nastáva až po zdvihnutí. Správe 200 OK SDP predchádzajú správy 100 traying, 180 ringing, PRACK, 200 OK na správu PRACK, potom pakety RTP/RTCP, ktoré rezervujú potrebnú šírku pásma a SDP relácie a potom nasleduje správa 200 OK SDP. Priemerná doba bez záťaže je 12 ms, s postupnou záťažou CSCF serverov táto doba rastie až na maximum pri záťaži CPU 100 % a RAM 75 % na 19,2 ms. V tabuľke vidíme, že percentuálny nárast času je väčší pri záťaži CPU 0 % a RAM 25 % ako pri CPU 100 % a RAM 25 % logicky vyplýva, že by to malo byť naopak, táto chyba je spôsobená nepresnosťami pri meraní a malým množstvom štatistických údajov použitých pri výpočte.

Tabuľka 13: Priemerná doba post pick up delay CPU 100 % RAM 0 % - 75 %

	Bez záťaže	So záťažou			
		CPU 100% RAM 0%	CPU 100% RAM 25%	CPU 100% RAM 50%	CPU 100% RAM 75%
Priemerná doba Post pick up delay[ms]	12	13,36	14,25	18,65	19,26
Percentuálny nárast [%]	0	11,3	18,75	55,4	60,5

Tabuľka 14: Priemerná doba post pick up delay CPU 0 % RAM 25 % - 75 %

	Bez záťaže	So záťažou		
		CPU 0 % RAM 25%	CPU 0% RAM 50%	CPU 0% RAM 75%
Priemerná doba Post pick up delay[ms]	12	15,65	15,69	16,35
Percentuálny nárast [%]	0	30,4	30,75	36,25

8.3.9 Session Disconnect Delay (SDD)

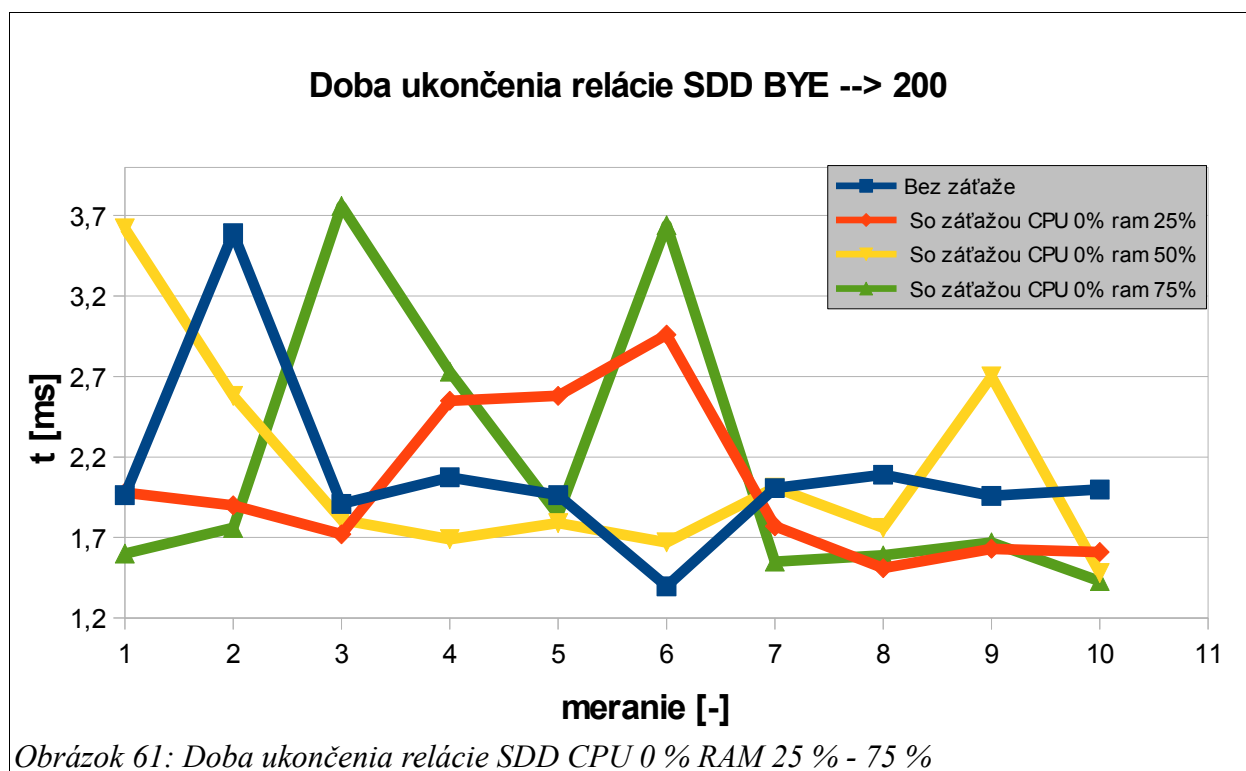
Tento parameter vyjadruje dobu ukončenia relácie, teda čas kedy je na správu BYE prijatá správa 200 OK.

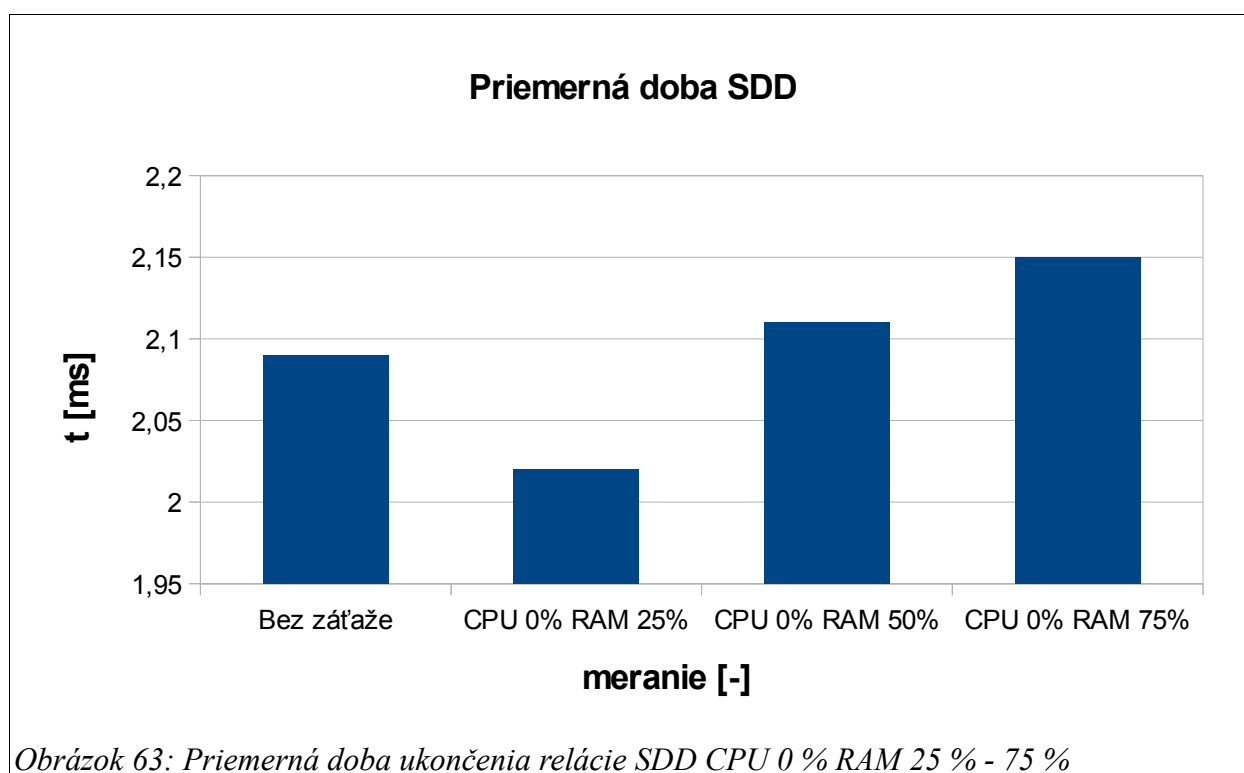
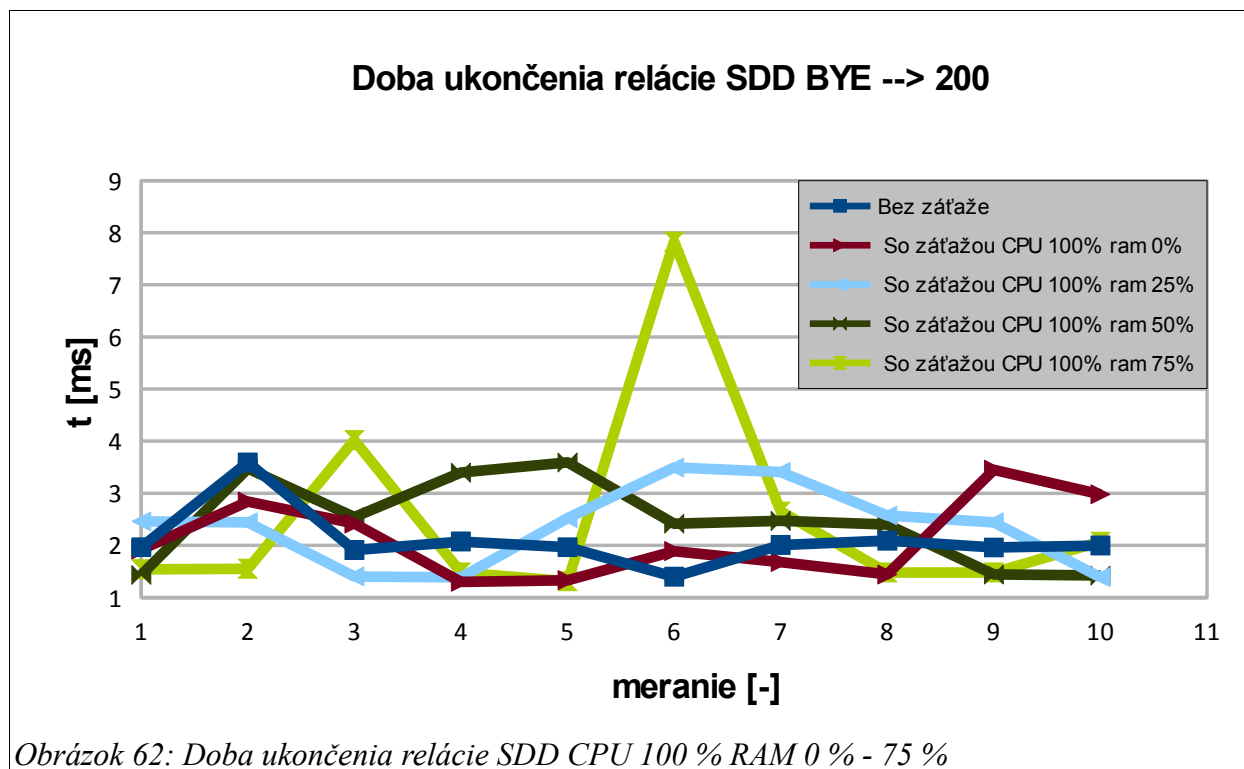
```

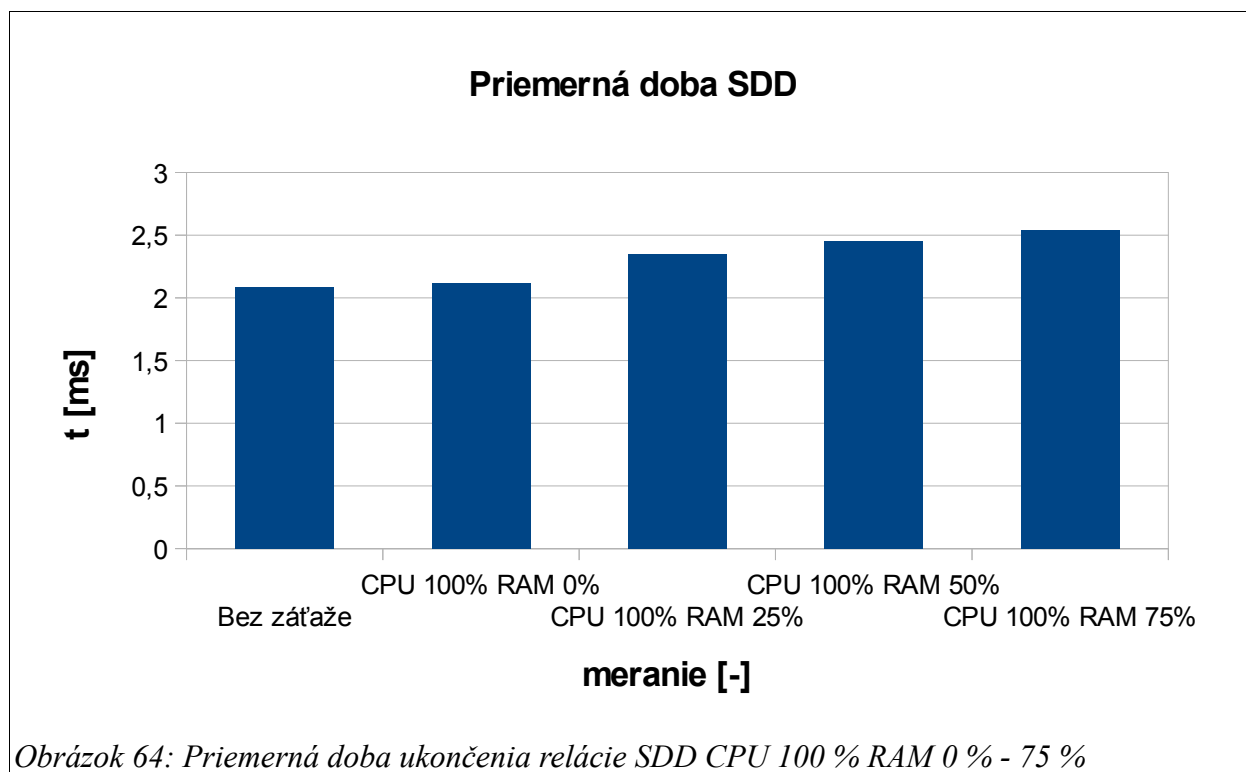
|Time      | 192.168.54.72      |
|          |          | 192.168.54.67      |
|25,275    |          | Request: BYE sip:bo |SIP: Request: BYE sip:bob@192.168.54.73:49516;transport=udp
|          | (59829)  -----> (4060) |
|25,276    |          | Status: 200 OK      |SIP: Status: 200 OK
|          | (59829)  <----- (4060) |

```

Obrázok 60: Flow graf, ukončenie relácie







Tento čas je definovaný ako čas medzi správou BYE a správou 200 OK. Vyjadruje, ako dlho trvá ukončenie relácie, ak volajúci alebo volaný požiada o ukončenie relácie. Priemerná hodnota bez záťaže je 2,09 ms a maximálna hodnota je 2,5 ms pri CPU 100 % a RAM 75 %. Priemerný čas pri CPU 0 % a RAM 25 % je menší ako bez záťaže, ale je vidieť, že ten rozdiel je len približne 0,07 ms, čo je dané nepresnosťami merania. Pri záťaži CPU 100 % a RAM 75 % šieste meranie je veľký skok času SDD a následný pokles, toto môže byť spôsobené spomínanou technológiou procesora, ktorý obsahovali CSCF servery.

Tabuľka 15: Priemerná doba ukončenia relácie SDD CPU 100 % RAM 0 % - 75 %

	Bez záťaže	So záťažou			
		CPU 100% RAM 0%	CPU 100% RAM 25%	CPU 100% RAM 50%	CPU 100% RAM 75%
Priemerná doba SDD[ms]	2,09	2,12	2,35	2,45	2,54
Percentuálny nárast [%]	0	1,43	12,4	17,2	21,5

Tabuľka 16: Priemerná doba ukončenia relácie SDD CPU 0 % RAM 25 % - 75 %

	Bez zátáže	So zátážou		
		CPU 0 % RAM 25%	CPU 0% RAM 50%	CPU 0% RAM 75%
Priemerná doba SDD[ms]	2,09	2,02	2,11	2,15
Percentuálny nárast [%]	0	-3,3	0,95	2,8

9 ZÁVER

Táto práca je zameraná na porozumenie architektúry IMS siete a jej testovaniu podľa dokumentu IETF RFC 6076, ktorý definuje základné metriky pre testovanie výkonnosti SIP protokolu v IMS sieti. Merané boli časy spracovania správ a odpovedí na správy pri vytváraní, ukončení relácie a pri prihlasovaní klienta do IMS siete. Metriky boli merané pri rôznej umelej záťaži procesora a operačnej pamäte. Podľa predpokladu sa so záťažou zvyšoval čas obsluhy a odpovedí správ. Záťaž bola rozložená v rozsahu CPU 0 – 99 % a RAM 0 – 95 % s krokom zvyšovania 25 % pre RAM. Avšak procesor bol zaťažený len 0 % a 99%, pretože pri záťaži 95% RAM malo toto zaťaženie väčší vplyv na systém ako maximálna záťaž procesora. Samozrejme, že nulové hodnoty neboli nulové, ale v rozmedzí 1 – 8 %. Tieto prostriedky spotrebovával systém na svoj chod. Ďalej je práca zameraná na návrh a realizáciu architektúry IMS siete a test-bedu pre túto sieť.

IMS je v súčasnosti veľmi prínosná ako pre mobilných operátorov, ako aj pre zákazníkov, pretože umožňuje konvergenciu pevných, mobilných sietí a Internetu, bez veľkých zásahov do architektúry existujúcich sietí. Táto technológia podporuje medzinárodné štandardy, je vysoko škálovateľná a zaručuje vysokú kvalitu služieb aj bezpečnosť siete. Riešenie IMS tiež pomáha prevádzkovateľom telekomunikačných sietí a poskytovateľom služieb rýchlo a ekonomicky zavádzať nové multimediálne služby, ktoré im prinesú ďalšie možnosti zisku. V Českej Republike bola po prvýkrát IMS integrovaná v roku 2007 do siete operátora Vodafone, spoločnosťou Ericsson.[20]

V práci opisujem funkcionality a úlohy jednotlivých uzlov a jednotlivé vrstvy architektúry IMS siete využívané protokoly pre signalizáciu, riadenie a autentifikáciu, návrh softvéru použitého na zostavenie IMS siete a návrh test-bedu pre testovanie výkonnosti end-to-end SIP protokolu.

Vo výsledkoch nie sú spracované hodnoty pri záťaži 95 % RAM, pretože pri tejto záťaži sieť nebola schopná spoľahlivo pracovať, dochádzalo k chybám a výpadkom serverov P – CSCF, S – CSCF a neschopnosť komunikácie HSS databázy so servermi a KPI pre prihlásenie do siete bolo veľmi malé. Pri ostatnej záťaži bolo toto KPI 100 %. Meranie bolo pre každú záťaž opakované 10-krát, môže sa to zdať málo pre dôveryhodné výsledky, ale podobný výkonnostný test pre IMS sieť bol realizovaný na Department of Electrical and Computer Engineering Illinois Institute of Technology Chicago a publikovaný v článku [13].

SIP protokol sa stal široko používaným štandardom medzi rôznymi poskytovateľmi služieb a užívateľov v telekomunikačnom priemysle a výrobcami komunikačných zariadení. Existovalo mnoho definovaných metrík pre testovanie výkonnosti iných komunikačných protokolov, ako napríklad SS7, avšak neexistovali žiadne definície pre testovanie SIP protokolu. Preto bolo vytvorené RFC 6076, ktoré tieto metriky definuje a poskytuje tak možnosti merania kvality služieb založených na SIP poskytovaných zákazníkom.

10 LITERATÚRA

[1]A.AHSON, S. - ILYAS, M.: IP Multimedia Subsystem (IMS) Handbook. 6000 Broken Sound Parkway NW, Suite 300, Florida : CRC Press Taylor & Francis Group, LLC, 2009. 562 s. ISBN 978-1-4200-6459-9

[2]AL-BEGAIN, Khalid, Chitra BALAKRISHNA, Luis Angel GALINDO a David MORO. *IMS: A Development and Deployment Perspective*. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom: John Wiley & Sons Ltd, 2009, 318 s. ISBN ISBN 978-0-470-74034-7 (H/B).

[3]AG PROJECTS. *OpenXCAP* [online]. 2010 [cit. 2012-11-19]. Dostupné z: <http://openxcap.org/>

[4]BAZOT, Philippe et al. IBM. *Developing SIP and IP Multimedia Subsystem (IMS) Applications*. IBM: IBM, 2007, 690 s. ISBN ISBN 0738489573.

[5] BYRD, M.: A Brief Introduction to IMS. International Engineering Consortium, 2006, [cit. 23.oct. 2012;17.59h CET]. Dostupné na webovskej stránke (world wide web):

http://www.iec.org/newsletter/sept06_1/broadband_1.html#top

[6] CAMARILLO, G. - A., M.: The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds, Second Edition. The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England : John Wiley & Sons Ltd, 2006. 423 s. ISBN 0-470-01818-6

[7]ETSI - European Telecommunications Standards Institute,
"Telecommunications and Internet converged Services and Protocols
for Advanced Networking (TISPAN): IMS/NGN Performance Benchmark, Part 1:
Core Concepts". ETSI TS 186 008-1. v1.1.1. Oct. 2007.

[8]ETSI - European Telecommunications Standards Institute,
"Telecommunications and Internet converged Services and Protocols
for Advanced Networking (TISPAN): IMS/NGN Performance Benchmark. Part 2:
Subsystem Configuration and Benchmarks". ETSI TS 186 008-2. v1.1.1. Oct.
2007.

- [9]ETSI - European Telecommunications Standards Institute, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN): IMS/NGN Performance Benchmark. Part 3: Traffic Sets and Traffic Profiles". ETSI TS 186 008-3. v1.1.1. Oct. 2007.". ETSI TS 186 008-3. Oct.2007
- [10]HANDA, Arun. *System Engineering for IMS networks*. Linacre House, Jordan Hill, Oxford OX2 8DP, UK: Newnes, 2009, 325 s. ISBN ISBN: 978-0-7506-8388-3.
- [11]IXIA - ENABLING A CONVERGED WORLD. *LxLoad* [online]. 2010 [cit. 2012-11-19]. Dostupné z: http://www.ixiacom.com/products/network_test/applications/ixload/index.php
- [12]KAMAILIO SIP SERVER PROJECT. *Kamailio open source SIP server* [online]. 2010 [cit. 2012-11-19]. Dostupné z: <http://www.kamailio.org/w/>
- [13]MALAS, D. a A. MORTON. INTERNET ENGINEERING TASK FORCE (IETF). *Request for Comments: 6076: Basic Telephony SIP End-to-End Performance Metrics*. January 2011
- [14]3rd Generation Partnership Project, "Universal Mo-bile Telecommunications System (UMTS), LTE, Telecommunication Management, Key Performance Indicators (KPI) for the IP Multimedia Subsystem (IMS)", 3GPP TS 32.454 (v. 10.0.0). Release 10.
- [15]OPEN IMS. *Open IMS Core* [online]. 2008 [cit. 2012-11-19]. Dostupné z: <http://www.openimscore.org/>
- [16]POIKSELKä, M. - MAYER, G.: *The IMS IP Multimedia Concepts and Services*, Third Edition. The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, United Kingdom : John Wiley & Sons Ltd, 2009. 533 s. ISBN 978-0-470-72196-4
- [17]POIKSELKÄ, Mikka, Georg MAYER a Hisham KHARTTABIL. *THE IMS IP: Multimedia Concepts and Services in the Mobile Domain*. West Sussex PO19 8SQ, England: John Wiley & Sons, Ltd, 2004, 450 s. ISBN ISBN 0-470-87113-X.
- [18]RUSSELL, T.: *The IP MULTIMEDIA SUBSYSTEM (IMS) Session Control and Other Network Operations*. United States of America : McGraw-Hill Companies, 2008. 242 s. ISBN 0-07-159464-7

[19]LOOKBUSY FREE SOFTWARE. *Lookbusy -- a synthetic load generator* [online]. 2010 [cit. 2012-11-25]. Dostupné z: <http://www.devin.com/lookbusy/>

[20]SVET KOMUNIKÁCIE. *Sieť IMS v Českej republike* [online]. 2007 [cit. 2012-11-25]. Dostupné z: <http://www.svet-komunikacie.sk/index.php?ID=3861s/installing-base-kamailio-ims-platform-debian-squeeze-32bit>

[21]TANG, Jin, Carol DAVIDS a Yu CHENG. A Study of An Open Source IP Multimedia Subsystem Test Bed. *Computer-Communication Networks*. 2008, č. 3.

[22]ŽILINSKÁ UNIVERZITA. *Network Information Library: Installing base Kamailio IMS platform on the debian squeeze - 32bit* [online]. 2010 [cit. 2012-11-25]. Dostupné z: <http://nil.uniza.sk/ngnims/kamailio-ims/installing-base-kamailio-ims-platform-debian-squeeze-32bit>

11 ZOZNAM ZKRATIEK

3G PP	Third Generation Partnership Project
AAA	Authentication Authorization and Accounting
AS	Appliction Server
ATM	Asynchronous Transfer Mode
B2BUA	Back-to-Back User Agent
BGCF	Breakout Gateway Control Function
CAMEL	Customized Applications for Mobile network Enhanced Logic
CAP	CAMEL Application Part
CS	Circuit Switched
CSCF	Call Session Function Control
DID	Direct inward dialing
DNS	Domain Name Server
DO	Design Objective
DOC	Design Objective Capacity
ENUM	Number Mapping
ETSI	European Telecommunications Standards Institute
GGSN	Gateway GPRS Support Node
GPRS	General packet radio service
GPU	General Public Licence
GSM	Global System for Mobile Communications
GSMSCF	GSM Service Control Function
HFC	Hybrid Fiber-Coaxial
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
iFC	Initial Filter Criteria
IM	Instant Messaging
IMPS	Instant Messaging and Presence Service
IMS	IP Multimedia Subsystem
IMS-ALG	IMS Application Layer Gateway
IP	Internet Protocol
IPsec	Internet Protocol Security
ISUP	ISDN User Part
IM-SSF	IP Multimedia Service Switching Function
LDAP	Lightweight Directory Access Protocol
MEGACO	Media Gateway Control Protocol
MGCF	Media Gateway Control Function
MGW	Media Gateway Function
MIME	Multipurpose Internet Mail Exxtensions
MRF	Media Resource Function
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
MSCF	Multimedia Service Control Function
MSRP	Message Session Relay Protocol
NGN	New Generation Network
OMA	Open Mobile Alliance
OSA-SCS	Open Service Access-Service Capability Server
PA	Presence Agent
PCM	Pulse Code Modulation

PDF	Policy Decision Function
PLMN	Public Land Mobile Network
PoC	Push to talk Over Cellular
PS	Packet Switched; Presence Server
PSTN	Public Switched Telephone Network
PUA	Presence User Agent
QoE	Quality of Experience
QoS	Quality of Service
RCS	Rapid Service Creation
RLS	Resource list Server
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SAPS	Scenario Attempts Per Second
SDP	Session Description Protocol
SEG	Security Gateway
SGW	Signalling Gateway
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol
SIMS	Simultaneous Scenario
SMTP	Simple Mail Transfer Protocol
SS7	Signaling System No.7
TCP	Transmission Control Protocol
TEM	Telecom Equipment Manufactures
THIG	Topology Hiding Inter-network Gateway
TrGW	Translation Gateway
TRT	Transaction respons Time
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
URI	Uniform Resource Identifier
WLAN	Wireless Local Area Network
XCAP	XML Configuration Access Protocol
XDMS	XML Document Management Sever
XML	Extensible Markup Language
XMLRPC	XML Remote Procedure Call